

NPS55LW73061A

NAVAL POSTGRADUATE SCHOOL

//

Monterey, California



NAVAL POSTGRADUATE SCHOOL

RANDOM NUMBER GENERATOR PACKAGE LLRANDOM

by

G. P. Learmonth

//
and

P. A. W. Lewis

June 1973

Approved for public release; distribution unlimited.

NAVAL POSTGRADUATE SCHOOL
Monterey, California

Rear Admiral M. B. Freeman
Superintendent

M. U. Clauser
Provost

ABSTRACT

This report is intended to describe an interim version of a computer program package for random number generation on the IBM System/360. The package, when called by a FORTRAN IV program, will deliver either a single value or an array (of specified size) of single precision uniformly, normally, or exponentially distributed pseudo-random deviates, or a single value or an array of uniformly distributed integers between 1 and $2^{31}-1$. The package also has the ability (optional) to "shuffle" the pseudo-random numbers to obtain "better" statistical properties.

Prepared by:

NAVAL POSTGRADUATE SCHOOL

RANDOM NUMBER GENERATOR PACKAGE LLRANDOM

I. Introduction	1
Some definitions	1
II. The Generator	3
A. Division simulation	6
B. Shuffling	7
C. Uniform (0.0,1.0) random numbers	9
D. Normally distributed random deviates	9
E. Exponential distribution	12
III. HOW TO USE THE PACKAGE	15
A. Implementation	18
B. Future Enhancements	20
References	21

Appendix of Program Listings

I. Introduction.

Numerous random number generators have been proposed for the System/360. Several of these generators have been incorporated into the subroutine library here at the Computer Center. The adequacy of some of these generators has rested on the results of some rather weak tests for randomness; recent results in the literature have shown many of these generators to be very poor performers. This report will describe an interim version of a package for random number generation which has stood up under intensive statistical testing and is deemed to be very satisfactory for the System/360. (The statistical testing will be reported elsewhere.)

The package, when called by a FORTRAN IV program, will deliver either a single value or an array (of specified size) of single precision, uniformly, normally, or exponentially distributed pseudo-random deviates or a single value or an array of pseudo-random integers uniformly distributed between 1 and $2^{31}-1$. The package also has the ability (optional) to "shuffle" the pseudo-random numbers to obtain "better" statistical properties.

Further refinements will be made to this generator; however, it is now available for use in an interim version under the name LLRANDOM. Future versions will be announced through the W. R. Church Computer Center Newsletter. The changes envisioned will be internal and aimed at increasing speed and efficiency of coding. The actual numbers produced in future versions will remain the same as described here, as will the FORTRAN calling sequence.

Some definitions. By "random number generator" or "pseudo-random number generator" is meant an algorithm by which sequences of numbers

are produced which follow a given probability distribution and possess the appearance of randomness. Without attempting to address the still unresolved philosophical question of what a random sequence is, the underlined words above are the keys to random number generation on a digital computer. The term sequence implies that many random numbers must be produced serially from the algorithm. The user may need only a very few of these numbers, however we generally require that the algorithm be able to produce very many numbers. Distribution implies that we can associate a probability statement with the occurrence of each random number. The distribution is usually taken to be uniform, that is, within a given range the probability of occurrence of a given number is the same as for any other number in a similar range. If the algorithm produces, say, m distinct numbers then the probability of occurrence for any one of them is $1/m$.

Lastly, we speak of the appearance of randomness. As will be shown next, the actual implementation of the algorithm is a recurrence relation where each succeeding number is a function of the preceding number. True randomness would require independence of successive numbers; however, the algorithm generates a deterministic sequence. Algorithms for random number generation do, however, yield sequences which appear to be random, hence the term "pseudo-random numbers." It is this characteristic which is the subject of statistical testing, that is, one asks, "how random does the given sequence appear?"

The uniform random number generator which forms the basis of the package described here is a Lehmer congruential generator. The recurrence relation is given by

$$X_n \equiv A \cdot X_{n-1} + C \pmod{m}. \quad (1)$$

This generator produces integer random numbers between 1 and m .

These integer values may then be transformed into real-valued numbers between 0.0 and 1.0 or into any desired distribution by an appropriate transformation.

II. The Generator.

The recurrence relation given in equation (1) is actually called a "Lehmer mixed congruential generator." The term mixed comes from the fact that it involves a multiplication by a constant, A , plus an addition of a constant, C . The actual implementation used in LLRANDOM is called a "multiplicative," or "pure," congruential generator in that we take $C = 0$, giving

$$X_n \equiv A \cdot X_{n-1} \pmod{m}. \quad (2)$$

The field of positive integers is, of course, infinite. It is a reality of digital computers that only a finite number of positive integers are expressible. Specifically, we are limited to the word size of the System/360. This word size is 32 bits with one bit reserved for the algebraic sign; hence, an obvious choice for m is 2^{31} . The product $A \cdot X_{n-1}$ is formed by the System/360 in two adjacent registers yielding a result which may be as large as 2^{63} . We must, however, reduce this product to a number less than or equal to 2^{31} . The mod, or modulo, operation accomplishes this. The product $A \cdot X_{n-1}$ is divided by 2^{31} leaving a quotient which is some multiple of 2^{31} and a remainder which is strictly less than 2^{31} . It is this remainder which is the next pseudo-random number X_n in the equation (1).

On first examination it would appear that a full 2^{31} numbers could be generated by the sequence (1). This is not the case, unless A and m are chosen properly. We define a term called the period which is the number of unique random numbers computable for a given choice of A and m . To illustrate the concept, assume we have a six-bit word with one bit for a sign. We then have $m = 2^5 = 32$. Choose $A = 9$ and work through a sequence starting with $X_0 = 1$.

Step n	X_{n-1}	$A \cdot X_{n-1}$	$A \cdot X_{n-1} \pmod{2^5}$
1	1	9	9
2	9	81	17
3	17	153	25
4	25	225	1
5	1	9	9
.	.	.	.
.	.	.	.
.	.	.	.

Note that the modulus of this generator is 32, however we have realized a period of only 4, that is the sequence of 1, 9, 17, 25, 1, 9, . . . repeats after only 4 numbers. Obviously, care must be taken to insure that such occurrences do not happen in a random number generator. Hopefully, the period will also be independent of the starting value, X_0 .

A great deal of work has been done on number theoretic considerations for the choice of m so as to yield a maximum period length (see Knuth³). To summarize, generators with modulus $m = 2^p$ for any integer, p , can have a maximum period of $m/4$, or, for the System/360, $2^{31}/4 = 2^{29}$; the period may also depend on the starting value. When the modulus m is a prime number, the maximum possible period is $m - 1$.

It so happens that the largest prime less than or equal to 2^{31} is $2^{31} - 1$, which is most fortuitous. Hence, choosing $m = 2^{31} - 1$ we can achieve a maximum period of $m - 1 = 2^{31} - 2$. These results produce only upper bounds on the period length. Recall in the example above, the maximum period possible is $2^5/4 = 2^3 = 8$, but that a period of only 4 was observed. This naturally leads to considerations of the choice of the multiplier, A .

Success in achieving a maximum period lies with the choice of the multiplier. Again, to briefly summarize the pertinent number theory, for a modulus 2^{31} the multiplier A must differ by 3 from the nearest multiple of 8; the starting value, X_0 , must be odd; A must be one greater than a multiple of 4; and C must be odd. These conditions only assure a maximum period of $m/4$, not necessarily good statistical properties. For the random number generator described here (LLRANDOM) we are choosing $C = 0$; hence, this length is not achievable if $m = 2^{31}$. Luckily, the conditions on choosing A for the modulus $m = 2^{31} - 1$ are more easily met and we can achieve the maximum period.

Utilizing some of the nice number theoretic properties of the number $2^{31} - 1$, to achieve a maximum period, A must be a positive primitive root of $2^{31} - 1$ or a power of such a number. This is generally not easy to find; the value of A used in the generator described here is 7^5 . The number 7 is a positive primitive root of $2^{31} - 1$ and raising 7 to the fifth power results in the multiplier 16807 which is also a positive primitive root of $2^{31} - 1$ (Lewis, Goodman, and Miller¹) and satisfies some conditions regarding the statistical performance of the generated sequence. These conditions will not be discussed here.

The generator

$$X_n \equiv 7^5 \cdot X_{n-1} \pmod{2^{31}-1} \quad (3)$$

is the generator reported in Lewis, Goodman, and Miller¹. The authors cite the results of very extensive tests on this generator, all of which show that it is very satisfactory.

A. Division simulation. A practical consideration for random number generators is that they be fast, hopefully without requiring excessive memory to achieve speed. In many applications rather large quantities of numbers are needed and the speed of the generator can be crucial.

Nearly all random number generators are coded as subroutine or function subprograms in the assembler or machine language of the computer. The algorithm for implementing (3) is rather simple, involving a multiplication and then a division to effect the modulo operation. On most computers the division operation is rather slow as compared to the multiplication operation. In the past, the multiplier A was chosen so that its binary representation contained many zeroes, thereby speeding the multiplication. Unfortunately, this choice was at the expense of the period length, since such multipliers rarely met the number theoretic conditions for a maximum period. For the LLRANDOM generator (3) described here, the division operation has been replaced by a division simulation involving two shifts and an add instruction. Should a fixed-point (integer) overflow occur, two more additions are required to correct the situation.

The ordinary division on a System/360 Model 67-2 requires 8.49 micro-seconds. Without overflow, the simulation requires only 3.45

micro-seconds. When overflow occurs, the simulation takes an additional 2.32 micro-seconds for a total of 5.77 micro-seconds. These overflows occur quite rarely, on the order of only once in 250,000 iterations.

The division simulation algorithm (again due to Lehmer) is discussed by Payne, Rabung, and Bogyo² and works as follows. Define a congruence relationship by

$$X'_n \equiv A \cdot X_{n-1} \pmod{2^{31}}. \quad (4)$$

Performing the modulo operation on the product AX_{n-1} would give

$$AX_{n-1} = q2^{31} + r, \quad (5)$$

where q is some quotient and r is the remainder and is strictly less than 2^{31} . Adding q to both sides of (4) we get

$$X_n = X'_n + q \equiv AX_{n-1} \pmod{2^{31}-1}. \quad (6)$$

This form gives the desired modulus of $2^{31} - 1$, if there is no overflow in the addition of $X'_n + q$. If there is overflow, to correct it we merely add a constant of 1 to get

$$X_n \equiv X'_n + q + 1 \pmod{2^{31}} = A \cdot X_{n-1} \pmod{2^{31}-1}, \quad (7)$$

which is again, the desired result.

This division simulation algorithm is very easily implemented on the System/360 and saves considerable execution time over conventional division.

B. Shuffling. The sequence produced by the generator (3) does appear to consist of independent, uniformly distributed numbers for most purposes.

We realize that the numbers are not actually independent, due to the procedure used to generate them. It has been proposed that a sequence of such numbers be further randomized, or "shuffled," to improve upon the appearance of randomness (see, for instance, Knuth³). Serial correlation tests are usually employed to detect lack of independence in a sequence and at least one generator, RANDU, known to perform badly in a three-dimensional serial test was improved by shuffling. These tests will be discussed elsewhere. The various shuffling procedures which have been put forward have had little empirical validation.

The package described here has a built-in shuffling mechanism and it works as follows. A table of 128 random integers is maintained in the package. The starting values in the table represent members of the sequence (3) lagged by one million integers starting with an arbitrary seed. When a new integer is generated by the algorithm, its right-most seven bits are masked-off to form an index into the table ($2^7=128$). The integer in the table indexed by the right-most seven bits is returned to the caller and that table entry is replaced by the integer just generated. In essence, we are taking "chunks" of 128 numbers from the basic sequence and shuffling them before they are used.

This particular shuffling scheme is dependent on the choice of the modulus. For a modulus of 2^{31} the right-most bits of a congruential random number generator are non-random and their use in this scheme would defeat the purpose of shuffling. However, with a modulus of $2^{31} - 1$ and the positive primitive root multiplier $A = 7^5$, the right-most bits are quite random and the desired results are obtained.

C. Uniform (0.0,1.0) random numbers. So far, we have discussed how to generate uniform random integers over the range 1 to $m = 2^{31} - 1$. In most applications, uniform random numbers over the range 0.0 to 1.0 are desired. In theory, the uniform integers, X_i , are divided by m to produce these numbers, as

$$U_i = X_i/m. \quad (8)$$

In actual implementation on the System/360, the integer result is algebraically shifted right seven bits and a normalized floating point exponent is logically OR'ed on to it. The result is a properly normalized floating point random number over the range 0.0 to 1.0, usually referred to as a "real" uniform number.

D. Normally distributed random deviates. The uniformly distributed random numbers described above are not only useful in their own right, but form the basis of transformations into random numbers with other probability distributions. One of the most important of these distributions is the Normal distribution.

There are several methods of approximating a Normal distribution with uniform random numbers. One of the oldest and, unfortunately, most common is the "sum of k uniforms method." The algorithm is based on the fact that the uniform (0.0,1.0) distribution has a mean of $1/2$ and a standard deviation of $\sqrt{1/12}$. The algorithm works as follows:

$$X = \frac{\sum_{i=1}^k U_i - k/2}{\sqrt{k/12.0}} \quad (9)$$

The random deviate X is approximately normally distributed with mean 0 and variance 1. The approximation is not as good as other methods and it is rather time consuming in that k uniforms must be generated and then summed. It was basically devised to overcome the very time consuming multiply and divide operations in older computers.

A more accurate algorithm is known as the Box-Muller method or Polar method which is actually a rejection method due to von Neumann. The method requires the generation of two uniforms to produce two independent Normals. It is based on the distribution of points inside the unit circle. The method is more accurate than the "sum of k uniforms method" (in fact, theoretically perfect). However, it does require two square roots and two natural logarithm operations which are generally rather time consuming.

The algorithm used in the package described here is based on a method developed by Marsaglia and is known as the "rectangle-wedge-tail" method. This algorithm is by far the fastest algorithm available for generating normally distributed random numbers, although it requires more memory than the Polar method.

The second volume of Knuth's "The Art of Computer Programming"³ gives a complete and detailed description of the algorithm. Briefly, the positive half of the Normal density curve is discretized into 37 rectangles, wedges, and a tail as in Figure 1. All of the rectangles are uniformly distributed densities. The wedges are approximated by "nearly linear densities." Finally, the tail distribution is computed by a modification to the Polar method. The normal density, $f(x)$, is then given by the composite function.

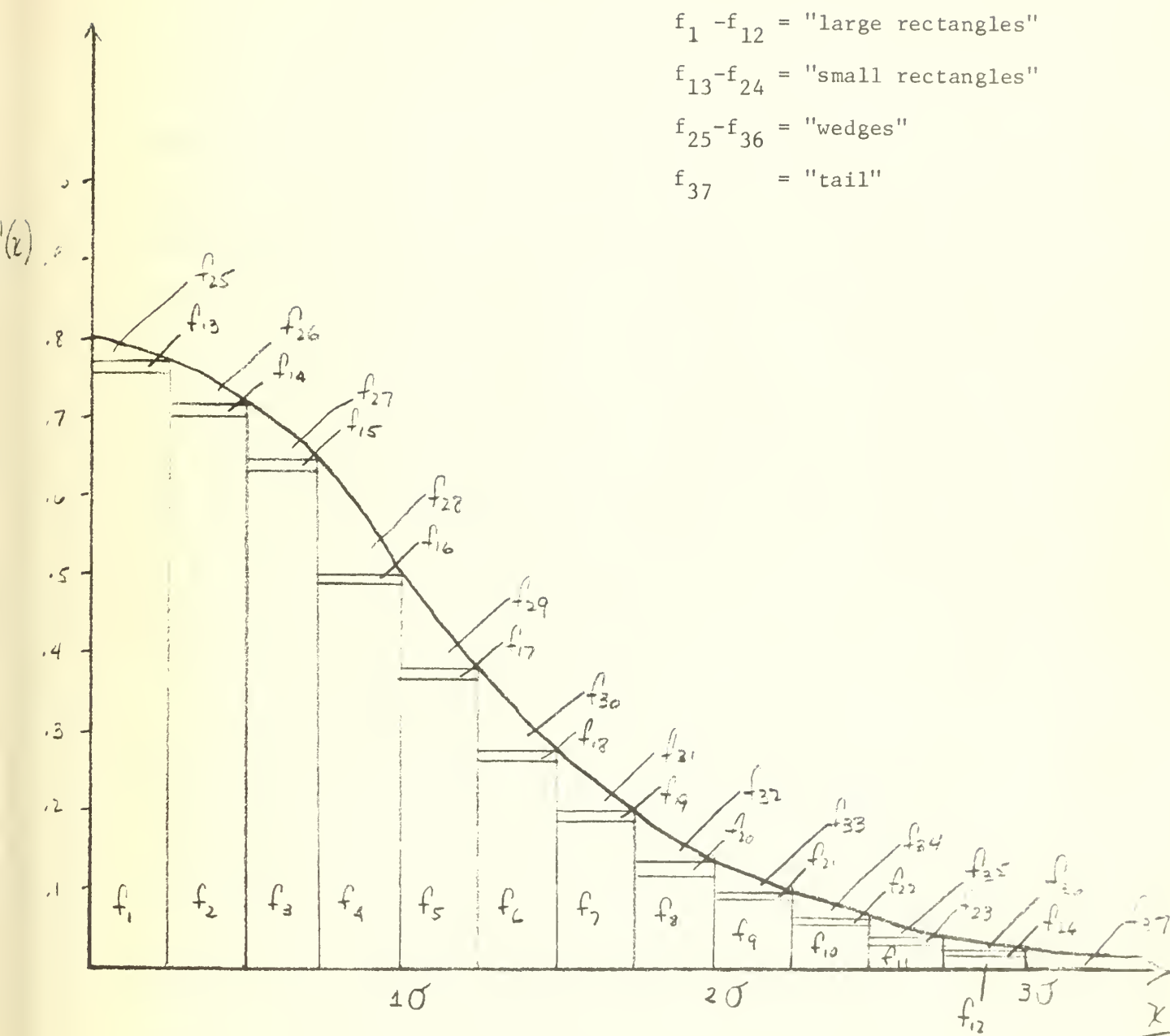


FIGURE 1

RECTANGLE-WEDGE-TAIL METHOD OF APPROXIMATING THE NORMAL DENSITY

$$f(x) = p_1 f_1(x) + p_2 f_2(x) + \dots + p_{37} f_{37}(x), \quad (10)$$

where

$$\sum_{i=1}^{37} p_i = 1,$$

the densities f_1 to f_{24} are the rectangles; f_{25} to f_{36} are the wedges; and f_{37} is the tail. The first twelve uniformly distributed rectangles are used 88% of the time. This makes for an extremely fast algorithm for the majority of deviates. When the tail is sampled, the deviate is generated by a modified Polar method and still quite satisfactory.

This generator for Normal deviates, like nearly all others, produces deviates with zero mean and unit variance. To change the scale and shape to any mean, μ , and the standard deviation, σ , we apply the linear transformation

$$Z = \mu + \sigma X \quad (11)$$

where z now has the desired shape and scale parameters.

E. Exponential distribution. Another probability distribution of major interest in simulations is the exponential. The cumulative distribution function and probability density function for the exponential are respectively

$$F(x) = 1 - e^{-\lambda x}, \quad (12)$$

$$f(x) = \lambda e^{-\lambda x}. \quad (13)$$

The expected value of the exponential distribution is:

$$E[X] = 1/\lambda. \quad (14)$$

The problem of generating exponential deviates reduces to one of generating "unit" exponentials, i.e. those with $\lambda = 1$, and then multiplying the result by whichever λ is necessary to give the desired distribution.

One of the most common methods of generating numbers from distributions other than the uniform is to use the inverse transformation technique (see Gaver and Thompson⁴). This can be described graphically, as in Figure 2, with a plot of the distribution function

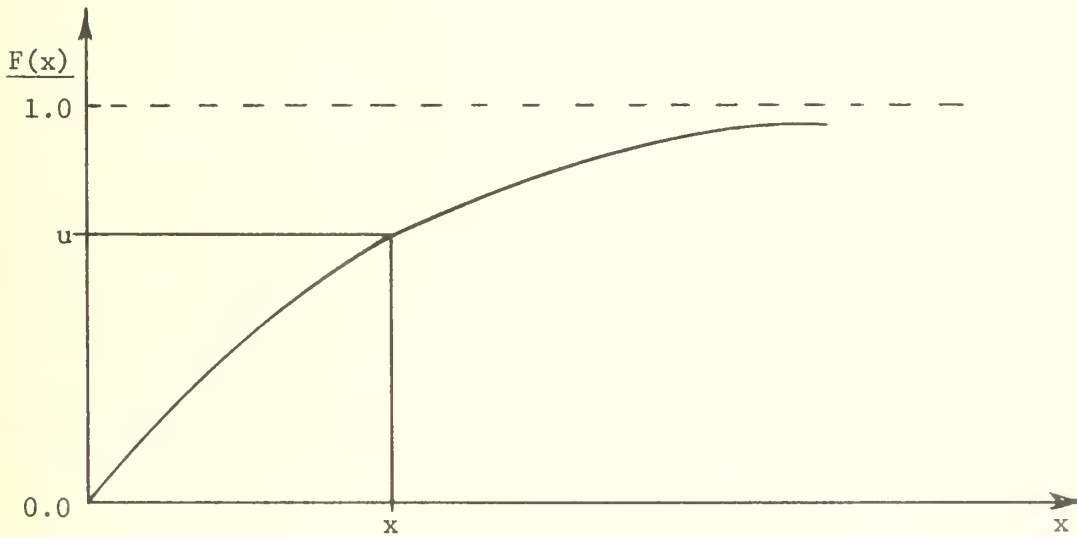


FIGURE 2.

CUMULATIVE DISTRIBUTION FUNCTION OF THE EXPONENTIAL DISTRIBUTION

The range of the abscissa, X , is infinite in extent. However, the range of the ordinate, $F(x)$, is $(0.0, 1.0)$, the range of uniform $(0,1)$ random variables. The inverse transformation technique is to generate a uniform random number, say U , and use this as the ordinate. The exponential deviate, say X , is the abscissa point corresponding to the intersection of the ordinate and the curve.

Mathematically, this technique is expressed as

$$u = F(x) = 1 - e^{-x}, \quad \lambda = 1, \quad (15)$$

$$x = F^{-1}(u),$$

where u is the uniform random number. This inverse transformation is rather easily implemented for exponentially distributed random variables via natural logarithms since we get

$$F^{-1}(U) = -\ln(1-U),$$

or by the symmetry of the uniform distribution

$$F^{-1}(U) = -\ln(U).$$

Perhaps the most common implementation of exponential deviate generators is this natural logarithm transformation. It is mathematically appealing as well as trivial to program, given the usual FORTRAN subroutines.

The exponential deviate generator in the LLRANDOM package is based on Marsaglia's method of dividing the probability density into a series of rectangles, wedges, and a tail. Although more complicated to program and larger in size, this method is approximately 40% faster than the logarithmic transformation.

For a survey of the generation of normal and exponentially distributed variables see Ahrens and Dieter⁵.

III. HOW TO USE THE PACKAGE.

The random number package described here is intended solely for use on the IBM System/360 or System/370 computers. The package consists of one Assembler F control section (CSECT) with nine entry points and two FORTRAN IV function subprograms. The names of the entry points and their functions are summarized in Table 1.

The subroutine entry point OVFLOW has no calling arguments and should be called once and only once at the beginning of the user's main FORTRAN program. The function subprograms RNORTH and REXPTH are called by the Assembler routine as needed and should not be called by the user. The eight additional entry points are the names of the actual routines to generate the random numbers. There are four types of random numbers which can be generated:

- (1) uniformly distributed integers on the range 1 to $2^{31} - 1$;
- (2) uniformly distributed single precision floating point numbers between 0.0 and 1.0;
- (3) single precision floating point normal deviates with mean zero and variance 1; and
- (4) single precision floating point exponential deviates with mean 1.

There is a separate entry point for each of the four types if shuffling of the sequence is desired.

For all eight entry points, the FORTRAN calling sequence is the same, namely:

```
CALL (entry point) (IX, A, N)
```

where

(entry point) refers to the routine desired,

viz. INT, SINT, RANDOM, SRAND, NORMAL, SNORM, EXPON, or SEXPON;

ENTRY POINT	FUNCTION
OVFLOW	Calls SPIE, handles fixed point overflows. (Must be called once at start of program.)
INT	Generates integer random numbers.
SINT	Generates shuffled integer random numbers.
RANDOM	Generates single precision floating point (0.0,1.0) random numbers.
SRAND	Generates single precision floating point (0.0,1.0) shuffled random numbers.
NORMAL	Generates single precision floating point normal deviates ($\mu=0, \sigma=1$).
SNORM	Generates shuffled single precision floating point normal deviates ($\mu=0, \sigma=1$).
EXPON	Generates single precision floating point exponential deviates ($\lambda=1$).
SEXPON	Generates shuffled single precision floating point exponential deviates ($\lambda=1$).

TABLE 1.

ENTRY POINT NAMES OF CONTROL SECTION OVFLOW

- IX is the starting value of the sequence and may contain any integer number between 1 and 2147483647. This variable should not be altered by the user during the execution of the program, unless it is desired to repeat a sequence of random numbers.
- A is either a scalar or vector variable and is the location with a specified dimension into which the random number or numbers are stored (see next parameter). Note that for entry points INT and SINT, this argument should be of INTEGER type.
- N is an integer variable or constant designating how many random numbers are to be generated during this call. If N is greater than 1, A above must be a vector dimensioned at least as large as N. If N is equal to 1, then A may be scalar.

Some sample programs are given below:

- (1) To generate 1000 consecutive integer random numbers:

```

INTEGER*4    M(1000)

CALL OVFLOW

IX = 1234567

--

--

--

CALL INT (IX, M, 1000)

--

END

```

- (2) To generate 25 shuffled single precision floating point normal deviates and scale to mean 10 and standard deviation 5:

```

REAL*4    A(25)

CALL OVFLOW

JJ = 1936748

N = 25

--

--

--

```



```

      CALL SNORM (JJ, A, N)

      DO 1 I = 1,25

      A(I) = A(I)*5.0 + 10.0

1  CONTINUE

      --
      --
      --

      END

(3) To generate one single precision floating point exponential
      deviate with mean 6:

      CALL OVFLOW

      I9 = 98367221

      --
      --
      --

      CALL EXPON (I9, E, 1)

      E = E*6.0

      --
      --
      --

      END

```

A. Implementation. LLRANDOM was designed and coded to run under Operating System/360 (OS). The Assembler Language control section contains a SPIE (Set Program Interrupt Exit) macro instruction which is a part of the OS Supervisor Services. This macro enables LLRANDOM to correct for the fixed point overflows resulting from the division simulation algorithm.

The remainder of the assembly coding is in Basic Assembler Language (BAL), i.e. no other macro calls or supervisor calls. To run LLRANDOM under another operating system for the System/360, an appropriate substitution for the SPIE macro would be necessary.

As currently programmed, LLRANDOM has the following memory requirements:

<u>MODULE</u>	<u>SIZE IN BYTES (DECIMAL)</u>
Assembler CSECT	3571
FORTTRAN function RNORTH	1512
FORTTRAN function REXPTH	<u>1106</u>
Total memory requirement	<u><u>6189</u></u>

The System/360 internal timer is rather crude for timing the execution of programs. The following times are therefore approximate timings for the generation of pseudo-random numbers on a System/360 Model 67-2.

<u>ENTRY POINT</u>	<u>TIME IN MICROSECONDS</u>
INT	10.7
SINT	15.7
RANDOM	15.6
SRAND	20.0
NORMAL	57.5 (Polar method takes 349 microseconds)
SNORM	65.8
EXPON	59.1 (Logarithm method takes 132 microseconds)
SEXPON	68.4

B. Future Enhancements. The normal and exponential deviate routines in LLRANDOM are patterned after a package, SUPER-DUPER, available from Professor G. Marsaglia at McGill University in Montreal. It is available at the Naval Postgraduate School. Marsaglia uses a different multiplier, A, and modulus, m, in his congruential generator from that used in LLRANDOM and he then exclusive OR's this result with the output of a feedback shift register generator. SUPER-DUPER provides only one deviate per call and does not provide for shuffling the sequence.

The two FORTRAN function subprograms, RNORTH and REXPTH, are taken (with slight modification) directly from SUPER-DUPER. Among the changes to be made to LLRANDOM will be to rewrite RNORTH and REXPTH in System/360 Assembly Language and incorporate them directly into the package.

We have experienced occasions where large-scale simulations have been coded in FORTRAN using double precision variables. The fact that LLRANDOM returns single precision numbers causes some inconvenience. To alleviate this problem we will provide the capability in LLRANDOM to return single precision numbers into double precision variables or arrays. Note that the values returned will still be single precision; however, they will be stored properly into double precision locations.

Finally, additional entry points will be added to provide single precision floating point gamma deviates. Shuffling of the gamma deviates will also be available.

Other enhancements are under consideration.

***** NAVAL POSTGRADUATE SCHOOL RANDOM NUMBER GENERATOR : LLRANDOM *****

```

C RNOR TOOTH FUNCTION
FUNCTION RNORTH(K,IX)
DIMENSION C(45)
DATA C/Z40FD2B5F,Z40FC2B5F,Z40FAA9AD,Z40F5A648,Z40F32496,
$ Z40EE2131,Z40E69C1A,Z40E198B5,Z40DA139E,Z40D28E87,Z40C887BE,
$ Z40C102A6,Z40B6FBDD,Z40ACF513,Z40A2EE4A,Z4098E78C,Z40916269,
$ Z40875BAC,Z407D54D6,Z40734E0D,Z406BC8F6,Z4061C22C,Z405A3D15,
$ Z4052B7FE,Z404B32E7,Z4043ADD0,Z403C28B9,Z40372554,Z402FA03D,
$ Z402A9CD8,Z40259973,Z4020960E,Z401E145C,Z401910F7,Z40168F45,
$ Z40140D93,Z40118BE0,Z3FF0A2E4,Z3FC887BE,Z3FA06C98,Z3F785172,
$ Z3F785172,Z3F50364C,Z3F50364C,Z3F79702E/
DATA I1/ZFBC35400/I2/ZFE79702E/
IF(K.GT.I1)GO TO 3
CALL RANDOM(IX,S,1)
CALL RANDCM(IX,T,1)
B=AINT(7.*(S+T))+37.*ABS(S-T)
CALL RANDOM(IX,Z9,1)
CALL RANDOM(IX,Z8,1)
X=Z9-Z8
RNORTH=.0625*(X+SIGN(B,X))
RETURN
IF(K.GT.I2)GO TO 5
CALL RANDOM(IX,Z9,1)
CALL RANDCM(IX,Z8,1)
IF(Z8.GT.0.50) Z9=-Z9
RNORTH=2.75*Z9
J=16.*ABS(RNORTH)+1.
IF(J-14) 6,6,7
P=(J+J-1)*.1497466E-2
GO TO 8
P=(89-J-J)*.698817E-3
CALL RANDCM(IX,Z9,1)
IF(Z9.GT.79.78846*(EXP(-.5*RNORTH*RNORTH))) GOTO4
$ -C(J)-P*(J-16.*ABS(RNORTH))) GOTO4
RETURN
CALL RANDOM(IX,V,1)
CALL RANDCM(IX,Z9,1)
IF(Z9.GT.0.5) V=-V
IF(V.EQ.0) GO TO 5
X=SQRT(7.5625-2.*ALOG(ABS(V)))
CALL RANDOM(IX,Z9,1)
IF(Z9*X.GT.2.75) GO TO 5
RNORTH=SIGN(X,V)
RETURN
END

```

3 4

6

7

8

5

RNOR0010
RNOR0020
RNOR0030
RNOR0040
RNOR0050
RNOR0060
RNOR0070
RNOR0080
RNOR0090
RNOR0100
RNOR0110
RNOR0120
RNOR0130
RNOR0140
RNOR0150
RNOR0160
RNOR0170
RNOR0180
RNOR0190
RNOR0200
RNOR0210
RNOR0220
RNOR0230
RNOR0240
RNOR0250
RNOR0260
RNOR0270
RNOR0280
RNOR0290
RNOR0300
RNOR0310
RNOR0320
RNOR0330
RNOR0340
RNOR0350
RNOR0360
RNOR0370
RNOR0380
RNOR0390
RNOR0400
RNOR0410
RNOR0420
RNOR0430
RNOR0440
RNOR0450

***** NAVAL POSTGRADUATE SCHOOL RANDOM NUMBER GENERATOR : LLRANDOM *****

```

OVFLOW      CSECT      RNORTH,REXPTH      LLRA0010
EXTRN       INT,SINT,RANDOM,SRAND,NORMAL,SNORM,EXPON,SEXPON LLRA0020
ENTRY       OVFLOW,R12      LLRA0030
USING       B      LLRA0040
            12(R15)      LLRA0050
            BRANCH AROUND ID      LLRA0060
            AL1(6)      LLRA0070
            CL6,OVFLOW,      LLRA0080
            R14,R12,12(R13)  SAVE REGISTERS IN HIGH SAVE AREA
            R12,R15      LLRA0090
            R13,SA+4      LLRA0100
            R2,R13      LLRA0110
            R13,SA      LLRA0120
            R13,8(R2)      LLRA0130
            NEW SAVE AREA      LLRA0140
            STORE WITH CALLING ROUTINE      LLRA0150
            LLRA0160
            LLRA0170
            LLRA0180
            LLRA0190
            LLRA0200
            LLRA0210
            LLRA0220

            ISSUE SPIE TO GET FIXED POINT OVERFLOWS AS WELL AS FORTRAN
            INTERRUPTS.

            SPIE      FIXIT,(8,9,12,13,15)
            ST      R1,PICA      SAVE FORTRAN'S PICA ADDRESS
            LM      R13,SA+4      RESTORE CALLER'S R13
            BCR     R14,R12,12(R13) RESTORE THE REGISTERS
            15,R14      RETURN

```

***** NAVAL POSTGRADUATE SCHOOL RANDOM NUMBER GENERATOR : LLRANDOM *****

```

*      SPIE BRINGS US HERE ON INTERRUPTS
*
*
*      FIXIT
      USING *,R15
      TM 7(R1),X'F7' WAS IT A FIXED POINT OVERFLOW?
      BC 5,FORT NO, LET FORTRAN'S SPIE HANDLE IT
      CLC 17(3,R1),AINT+1 TEST WHETHER BASE OF INTERRUPTED
      BL 0(,R14) ROUTINE WAS BETWEEN ENTRIES INT AND
      CLC 17(3,R1),ASEXPO+1 SEXPON INCLUSIVE; IF NOT, IGNORE
      BH 0(,R14) THE INTERRUPT
      A ADD 2**31-3
      AR R4,PM2 ADD 4 MORE TO MAKE 2**31+1 CORRECTION
      BR R4,R2 ADD 4 MORE TO MAKE 2**31+1 CORRECTION
      L R14 ALL FIXED, CONTINUE
      L R15,PICA NOT EXTENDED, POINT OVERFLOW, LET FORTRAN
      BR R15,0(,R15) EXTENDED ERROR HANDLING ROUTINE
      BR R15 TAKE CARE OF IT

      FORT

```

LLRA0240
 LLRA0250
 LLRA0260
 LLRA0270
 LLRA0280
 LLRA0290
 LLRA0300
 LLRA0310
 LLRA0320
 LLRA0330
 LLRA0340
 LLRA0350
 LLRA0360
 LLRA0370
 LLRA0380
 LLRA0390

***** NAVAL POSTGRADUATE SCHOOL RANDOM NUMBER GENERATOR : LLRANDOM *****

```

** *
ENTRY POINT : INT
      CNOP 0,8
      USING INT,R15
      B 8(R15)
      DC AL1(3)
      DC CL3,INT,
      STM R14,R12,12(R13)
      ST R13,SA+4
      LR R2,R13
      LA R13,SA
      ST R13,8(R2)
      L R9,A75
      LA R2,4
      LM R5,R7,0(R1)
      L R5,0(R5)
      L R3,0(R7)
      SLA R3,2
      SR R6,R2
      LR R7,R2
      CNOP 0,8
      MR R4,R9
      SLDA R4,1
      SRL R5,1
      AR R4,R5
      LR R5,R4
      ST R5,0(R7,R6)
      BXLE R7,R2,L1
      L R4,0(R1)
      ST R5,0(R4)
      L R13,SA+4
      LM R14,R12,12(R13)
      BCR 15,R14
      RETURN

      BASE REGISTER
      BRANCH AROUND ID

      SAVE REGISTERS IN HIGH SAVE AREA
      ADDRESS OF HIGH SAVE AREA IN LOW SAVE AR.
      COPY TO R2
      ADDRESS OF LOW SAVE AREA IN HIGH SAVE AR.
      LOAD MULTPLIER
      CONSTANT FOR BXLE
      ADDRESSES OF THREE ARGUMENTS
      LOAD STARTING VALUE INTO R5
      NUMBER OF CONSECUTIVE WORDS TO FILL
      CONVERT TO BYTES
      BACKUP ONE WORD IN CALLER'S ARRAY
      INITIAL VALUE FOR INDEX REGISTER
      ALIGN BXLE LOOP FOR SPEED
      FORM PRODUCT OF A AND X(N-1)
      R4= REMAINDER ; R5 = QUOTIENT THEREBY
      ADD QUOTIENT TO REMAINDER BY 2*31-1
      PUT X(N) INTO R5 FOR NEXT GC AROUND
      STORE IN CALLER'S ARRAY
      LOOP AROUND AGAIN
      GET STARTING VALUE ADDRESS AGAIN
      STORE AS STARTING VALUE FOR NEXT CALL
      RESTORE CALLER'S SAVE AREA POINTER
      RESTORE THE REGISTERS

```

LLRA0410
 LLRA0420
 LLRA0430
 LLRA0440
 LLRA0450
 LLRA0460
 LLRA0470
 LLRA0480
 LLRA0490
 LLRA0500
 LLRA0510
 LLRA0520
 LLRA0530
 LLRA0540
 LLRA0550
 LLRA0560
 LLRA0570
 LLRA0580
 LLRA0590
 LLRA0600
 LLRA0610
 LLRA0620
 LLRA0630
 LLRA0640
 LLRA0650
 LLRA0660
 LLRA0670
 LLRA0680
 LLRA0690
 LLRA0700
 LLRA0710
 LLRA0720
 LLRA0730
 LLRA0740

L1

N1

***** NAVAL POSTGRADUATE SCHOOL RANDOM NUMBER GENERATOR : LLRANDOM *****

```

*      ENTRY POINT : SINT
*      *
*      SINT
      CNOP      0,8
      USING     SINT,R15
      B         10(0,R15)
      DC        AL1(4)
      DC        CL4,SINT
      STM       R14,R12,12(R13)
      ST        R13,SA+4
      LR        R2,R13
      LA        R13,SA
      ST        R13,8(R2)
      LA        R9,A75
      LM        R2,4
      L         R5,R7,0(R1)
      L         R5,0(R5)
      L         R3,0(R7)
      L         R3,2
      SR        R6,R2
      LR        R7,R2
      LA        R8,TABLE
      L         R1,MASK
      CNOP      0,8
      MR        R4,R9
      SLDA      R4,1
      SRL       R5,1
      AR        R4,R5
      LR        R5,R4
      NR        R4,R1
      SLA       R4,2
      L         R0,0(R4,R8)
      ST        R5,0(R4,R8)
      ST        R0,0(R7,R6)
      BXL      R7,R2,L2
      L         R13,SA+4
      L         R1,24(R13)
      L         R4,0(R1)
      ST        R5,0(R4)
      LM        R14,R12,12(R13)
      BCR      15,R14

      BASE REGISTER
      BRANCH AROUND ID

      SAVE REGISTERS IN HIGH SAVE AREA
      ADDRESS OF HIGH SAVE AREA IN LOW SAVE AR.
      COPY TO R2
      ADDRESS OF LOW SAVE AREA
      LOAD MULTIPLIER
      CONSTANT FOR BXLE
      ADDRESSES OF THREE ARGUMENTS
      LOAD STARTING VALUE INTO R5
      NUMBER OF CONSECUTIVE WORDS TO FILL
      CONVERT TO BYTES
      BACKUP ONE WORD IN CALLER'S ARRAY
      INITIAL VALUE FOR INDEX REGISTER
      ADDRESS OF SHUFFLING TABLE
      INDEX MASK FOR SHUFFLING
      ALIGN BXLE LOOP FOR SPEED
      FORM PRODUCT OF A AND X(N-1)
      R4 = REMAINDER ; R5 = QUOTIENT
      ADD QUOTIENT TO REMAINDER THEREBY
      PUT X(N) INTO R5 FOR NEXT GC AROUND
      EXTRACT RIGHT-MOST 7 BITS
      CONVERT TO BYTE OFFSET IN TABLE
      SELECT RANDOM TABLE VALUE
      REPLACE TABLE VALUE WITH X(N)
      RANDOM TABLE VALUE TO CALLER'S ARRAY
      LOOP AROUND AGAIN
      RESTORE CALLER'S SAVE AREA POINTER
      GET ARGUMENT LIST POINTER AGAIN
      GET STARTING VALUE ADDRESS AGAIN
      STORE AS STARTING VALUE FOR NEXT CALL
      RESTORE THE REGISTERS
      RETURN

```

LLRA0760
LLRAC770
LLRA0780
LLRAC790
LLRA0800
LLRA0810
LLRA0820
LLRA0830
LLRA0840
LLRA0850
LLRA0860
LLRA0870
LLRA0880
LLRA0890
LLRA0900
LLRA0910
LLRA0920
LLRA0930
LLRA0940
LLRA0950
LLRA0960
LLRA0970
LLRA0980
LLRA0990
LLRA1000
LLRA1010
LLRA1020
LLRA1030
LLRA1040
LLRA1050
LLRA1060
LLRA1070
LLRA1080
LLRA1090
LLRA1100
LLRA1110
LLRA1120
LLRA1130
LLRA1140
LLRA1150
LLRA1160

***** NAVAL POSTGRADUATE SCHOOL RANDOM NUMBER GENERATOR : LLRANDOM *****

* * *

ENTRY PCINT : RANDOM

RANDOM

```

CNOP C,8
USING RANDOM,R15
B 12(,R15)
DC AL1(6)
DC CL6,RANDOM*
STM R14,R12,12(R13)
STR R13,SA+4
LA R13,SA
STR R13,8(,R2)
LM R9,R11,A75
LA R2,4
LM R5,R7,0(R1)
L R5,0(,R5)
L R3,0(,R7)
SLA R3,2
SR R6,R2
LR R7,R2
SUR FRO,FRO
LA R12,N3
LA R13,M3
CNOP O,8
MR R4,R9
SLDA R4,1
SRL R5,1
AR R4,R5
LR R5,R4
SRL R4,7
OR R4,R10
STR R4,0(R7,R6)
BCR R4,R11
BXLE R7,R2,L3
LST R4,0(,R1)
LM R5,0(,R4)
LM R13,SA+4
LM R14,R12,12(R13)
LM R15,R14
BCR FR2,0(R7,R6)
LEA FR2,FRO
STE FR2,0(R7,R6)
BR R12

```

L3

N3

M3

BASE REGISTER
BRANCH AROUND ID

```

SAVE REGISTERS IN HIGH SAVE AREA
ADDRESS OF HIGH SAVE AREA IN LOW SAVE AR.
COPY TO R2
ADDRESS OF LOW SAVE AREA
ADDRESS OF LOW SAVE AREA IN HIGH SAVE AR.
LOAD MULTIPLIER AND NORMALIZATION CONST.
CONSTANT FOR BXLE
ADDRESSES OF THREE ARGUMENTS
LOAD STARTING VALUE INTO R5
NUMBER OF CONSECUTIVE WORDS TO FILL
CONVERT TO BYTES
BACKUP ONE WORD IN CALLER'S ARRAY
INITIAL VALUE FOR INDEX REGISTER
CLEAR FLOATING POINT REGISTER 0
ADDRESS OF BXLE INSTRUCTION
ADDRESS OF NORMALIZATION ROUTINE
ALIGN BXLE LOOP FOR SPEED
FORM PRODUCT OF A AND X(N-1)
R4 = REMAINDER ; R5 = QUOTIENT
ADD QUOTIENT TO REMAINDER THEREBY
SIMULATING DIVISION BY 2**31-1
PUT X(N) INTO R5 FOR NEXT GO AROUND
MAKE ROOM FOR THE EXPONENT
OR ON THE EXPONENT
STORE IN CALLER'S ARRAY
DID IT NEED NORMALIZATION?
YES, GO NORMALIZE IT
LOOP AROUND AGAIN
GET STARTING VALUE ADDRESS AGAIN
STORE AS STARTING VALUE FOR NEXT CALL
RESTORE CALLER'S SAVE AREA POINTER
RESTORE THE REGISTERS
RETURN
LOAD INTO FLOATING POINT REGISTER 2
ADD ZERO AND NORMALIZE
STORE BACK NORMALIZED
CONTINUE THE BXLE LOOP

```

LLRA1180
LLRA1190
LLRA1200
LLRA1210
LLRA1220
LLRA1230
LLRA1240
LLRA1250
LLRA1260
LLRA1270
LLRA1280
LLRA1290
LLRA1300
LLRA1310
LLRA1320
LLRA1330
LLRA1340
LLRA1350
LLRA1360
LLRA1370
LLRA1380
LLRA1390
LLRA1400
LLRA1410
LLRA1420
LLRA1430
LLRA1440
LLRA1450
LLRA1460
LLRA1470
LLRA1480
LLRA1490
LLRA1500
LLRA1510
LLRA1520
LLRA1530
LLRA1540
LLRA1550
LLRA1560
LLRA1570
LLRA1580
LLRA1590
LLRA1600
LLRA1610
LLRA1620


```

** *
ENTRY POINT :  SRAND
                G,8
CNOPI SRAND,R15
USING 10(,R15)
B      AL1(5)
DC     CL5,SRAND,
DC     R13,SA+4
STM    R13,SA
ST      R2,R13
L      R13,SA
LA      R13,8(,R2)
ST      R9,R11,A75
LM      R2,4
LA      R5,R7,0(R1)
LM      R5,0(,R5)
L      R3,0(,R7)
L      R3,2
SLA     R6,R2
SR      R7,R2
SUR     FR0,FR0
LA      R12,N4
LA      R13,M4
LA      R8,TABLE
L      R1,MASK
CNOPI 0,8
MR      R4,R9
SLDA    R4,1
SRL     R5,1
AR      R4,R5
LR      R5,R4
NR      R4,R1
SLA     R4,2
L      R0,0(R4,R8)
SRL     R5,0(R4,R8)
R0,7
OR      R0,R10
ST      R0,0(R7,R6)
CR      R0,R11
BCR     4,R13
BXLE    R7,R2,L4
L      R13,SA+4
L      R1,24(,R13)
L      R4,0(,R1)
ST      R5,0(,R4)
LM      R14,R12,12(R13)
BCR     15,R14
LE      FR2,0(R7,R6)

                SRAND,R15
                BRANCH AROUND ID
                SAVE REGISTERS IN HIGH SAVE AREA
                ADDRESS OF HIGH SAVE AREA IN LOW SAVE AR.
                COPY TO R2
                ADDRESS OF LOW SAVE AREA
                LOAD MULTIPLIER AND NORMALIZATION CONST.
                CONSTANT FOR BXLE
                ADDRESSES OF THREE ARGUMENTS
                LOAD STARTING VALUE INTO R5
                NUMBER OF CONSECUTIVE WORDS TO FILL
                CONVERT TO BYTES
                BACKUP ONE WORD IN CALLER'S ARRAY
                INITIAL VALUE FOR INDEX REGISTER
                CLEAR FLOATING POINT REGISTER 0
                ADDRESS OF BXLE INSTRUCTION
                ADDRESS OF NORMALIZATION ROUTINE
                INDEX MASK FOR SHUFFLING
                ALIGN BXLE LOOP FOR SPEED
                FORM PRODUCT OF A AND X(N-1)
                R4 = REMAINDER ; R5 = QUOTIENT THEREBY
                ADD QUOTIENT TO REMAINDER BY 2**31-1
                PUT X(N) INTO R5 FOR NEXT GC AROUND
                EXTRACT RIGHT-MOST 7 BITS
                CONVERT TO BYTE OFFSET IN TABLE
                SELECT RANDOM TABLE VALUE
                REPLACE TABLE VALUE WITH X(N)
                MAKE ROOM FOR THE EXPONENT
                OR ON THE EXPONENT
                STORE IN CALLER'S ARRAY
                DID IT NEED NORMALIZATION ?
                YES, GO NORMALIZE IT
                LOOP AROUND AGAIN
                RESTORE CALLER'S SAVE AREA POINTER
                GET ARGUMENT LIST POINTER AGAIN
                GET STARTING VALUE ADDRESS AGAIN
                STORE AS STARTING VALUE FOR NEXT CALL
                RESTORE THE REGISTERS
                RETURN
                LOAD INTO FLOATING POINT REGISTER 2

```

LLRA1640
LLRA1650
LLRA1660
LLRA1670
LLRA1680
LLRA1690
LLRA1700
LLRA1710
LLRA1720
LLRA1730
LLRA1740
LLRA1750
LLRA1760
LLRA1770
LLRA1780
LLRA1790
LLRA1800
LLRA1810
LLRA1820
LLRA1830
LLRA1840
LLRA1850
LLRA1860
LLRA1870
LLRA1880
LLRA1890
LLRA1900
LLRA1910
LLRA1920
LLRA1930
LLRA1940
LLRA1950
LLRA1960
LLRA1970
LLRA1980
LLRA1990
LLRA2000
LLRA2010
LLRA2020
LLRA2030
LLRA2040
LLRA2050
LLRA2060
LLRA2070
LLRA2080
LLRA2090
LLRA2100
LLRA2110
LLRA2120

L4

N4

M4

***** NAVAL POSTGRADUATE SCHOOL RANDOM NUMBER GENERATOR : LLRANDOM *****

AER	FR2,FRO	ADD ZERO AND NORMALIZE	LLRA2130
STE	FR2,0(R7,R6)	STORE BACK NORMALIZED	LLRA2140
BR	R12	CONTINUE THE BXLE LOOP	LLRA2150

```

* * * ENTRY PCINT : NORMAL
NORMAL
CNP0 0,8
USING NORMAL,R15
B 12(,R15)
DC AL1(6)
DC CL6,NORMAL
STM R14,R12,12(R13)
ST R13,SA2+4
LR R2,R13
LA R13,SA2
ST R13,8(,R2)
LM R9,R11,A75N
LA R2,4
LM R5,R7,0(R1)
L R5,0(,R5)
L R3,0(,R7)
SLA R3,2
SR R6,R2
LR R7,R2
LA R13,ATBLE
LA R12,N5
CNP0 0,8
MR R4,R9
SLDA R4,1
SRL R5,1
AR R4,R5
LR R5,R4
LR R0,R5
LR R4,R11
BC 8,F1
LNR R5,R5
SLR R4,R4
CL R5,C1
BC 11,F2
SLDL R4,8
IC R4,0(R4,R13)
STC R4,PWRD+1
SRL R5,8
ALR R5,R10
ST R5,0(R7,R6)
LE FRO,PWRD
AE FRO,0(R7,R6)
STE FRO,0(R7,R6)
LR R5,R0
BR R12
CL R5,C2
BC 11,F3
LLRA2170
LLRA2180
LLRA2190
LLRA2200
LLRA2210
LLRA2220
LLRA2230
LLRA2240
LLRA2250
LLRA2260
LLRA2270
LLRA2280
LLRA2290
LLRA2300
LLRA2310
LLRA2320
LLRA2330
LLRA2340
LLRA2350
LLRA2360
LLRA2370
LLRA2380
LLRA2390
LLRA2400
LLRA2410
LLRA2420
LLRA2430
LLRA2440
LLRA2450
LLRA2460
LLRA2470
LLRA2480
LLRA2490
LLRA2500
LLRA2510
LLRA2520
LLRA2530
LLRA2540
LLRA2550
LLRA2560
LLRA2570
LLRA2580
LLRA2590
LLRA2600
LLRA2610
LLRA2620
LLRA2630
LLRA2640
LLRA2650
BASE REGISTER
BRANCH AROUND ID
SAVE REGISTERS IN HIGH SAVE AREA
ADDRESS OF HIGH SAVE AREA IN LOW SAVE AR.
COPY TO R2
ADDRESS OF LOW SAVE AREA IN HIGH SAVE AR.
LOAD MULTIPLIER, EXPONENT, AND TEST MASK
CONSTANT FOR BXLE
ADDRESSES OF THREE ARGUMENTS
LOAD STARTING VALUE INTO R5
NUMBER OF CONSECUTIVE WORDS TO FILL
CONVERT TO BYTES
BACKUP ONE WORD IN CALLER'S ARRAY
INITIAL VALUE FOR INDEX REGISTER
ADDRESS OF TABLE OF CONSTANTS
ADDRESS OF BXLE
ALIGN BXLE LOOP FOR SPEED
FORM PRODUCT OF A AND X(N-1)
R4 = REMAINDER ; R5 = QUOTIENT
ADD REMAINDER TO REMAINDER THEREBY
PUT X(N) INTO R5
COPY R5 INTO R0 FOR NOW
SHOULD WE MAKE IT NEGATIVE ?
POSITIVE, KEEP GOING
MAKE R5 TRUE NEGATIVE
CLEAR R4 TO ZERO
R5 LESS THAN X'68000000' ?
NO
SHIFT FIRST 8 BITS OF R5 INTO R4 AS INDEX
OBTAIN CONSTANT FROM TABLE
STORE IN SECOND BYTE OF PWRD
SHIFT REMAINING 24 BITS RIGHT THEN OR ON
EXPONENT TO MAKE (24 BITS)/16
STORE IN CALLER'S ARRAY
LOAD CHARACTERISTIC TO FLOATING POINT
REGISTER 0 AND ADD FRACTION
STORE NORMAL DEViate IN CALLER'S ARRAY
COPY BACK TO R5 FOR NEXT GO AROUND
GO TO BXLE AND CCNTINUE
R5 LESS THAN X'D0000000' ?
NO

```

L5

F1

F2

F3	SLDL	R4,8	SHIFT FIRST 8 BITS OF R5 INTO R4 AS INDEX	LLRA2660
	SL	R4,C1M	SUBTRACT 68	LLRA2670
	IC	R4,0(R4,R13)	OBTAIN CONSTANT FROM TABLE	LLRA2680
	STC	R4,0(NWRD+1)	STORE IN SECOND BYTE OF NWRD	LLRA2690
	SRL	R5,8	SHIFT REMAINING 24 BITS RIGHT THEN OR ON	LLRA2700
	ALR	R5,R10	EXPONENT TO MAKE $\cdot (24 \text{ BITS})/16$	LLRA2710
	ST	R5,0(R7,R6)	STORE IN CALLER'S ARRAY	LLRA2720
	LE	R5,0(NWRD)	LOAD CHARACTERISTIC TO FLOATING POINT	LLRA2730
	STE	FR0,0(R7,R6)	REGISTER 0 AND SUBTRACT FRACTION	LLRA2740
	LR	FR0,0(R7,R6)	STORE NORMAL DEVIATE IN CALLER'S ARRAY	LLRA2750
	CL	R5,R0	COPY BACK TO R5 FOR NEXT GC AROUND	LLRA2760
	BC	R12	GO TO BXLE AND CONTINUE	LLRA2770
	SLDL	R5,C3	R5 LESS THAN X'E2F00000' ?	LLRA2780
	SL	11,F4	NO	LLRA2790
	IC	R4,12	SHIFT FIRST 12 BITS OF R5 INTO R4	LLRA2800
	STC	R4,C2M	SUBTRACT CE8	LLRA2810
	SRL	R4,0(R4,R13)	OBTAIN CONSTANT FROM TABLE	LLRA2820
	ALR	R4,0(PWRD+1)	STORE IN SECOND BYTE OF PWRD	LLRA2830
	ST	R5,8	SHIFT REMAINING 20 BITS RIGHT THEN OR ON	LLRA2840
	LE	R5,R10	EXPONENT TO MAKE $\cdot (20 \text{ BITS})/16$	LLRA2850
	AE	FR0,0(R7,R6)	LOAD CHARACTERISTIC TO FLOATING POINT	LLRA2860
	STE	FR0,0(PWRD)	REGISTER 0 AND ADD FRACTION	LLRA2870
	LR	FR0,0(R7,R6)	STORE NORMAL DEVIATE IN CALLER'S ARRAY	LLRA2880
	CL	R5,RC	COPY BACK TO R5 FOR NEXT GC AROUND	LLRA2890
	BC	R12	GO TO BXLE AND CONTINUE	LLRA2900
	SLDL	R5,C4	R5 LESS THAN X'F5E00000' ?	LLRA2910
	SL	11,F5	NO	LLRA2920
	IC	R4,12	SHIFT FIRST 12 BITS OF R5 INTO R4	LLRA2930
	STC	R4,C3M	SUBTRACT E17	LLRA2940
	SRL	R4,0(R4,R13)	OBTAIN CONSTANT FROM TABLE	LLRA2950
	ALR	R4,0(NWRD+1)	STORE AS SECOND BYTE OF NWRD	LLRA2960
	ST	R5,8	SHIFT REMAINING 20 BITS RIGHT THEN OR ON	LLRA2970
	LE	R5,R10	EXPONENT TO MAKE $\cdot (20 \text{ BITS})/16$	LLRA2980
	STE	FR0,0(R7,R6)	STORE IN CALLER'S ARRAY	LLRA2990
	LR	FR0,0(NWRD)	LOAD CHARACTERISTIC TO FLOATING POINT	LLRA3000
	CL	FR0,0(R7,R6)	REGISTER 0 AND SUBTRACT FRACTION	LLRA3010
	BC	FR0,0(R7,R6)	STORE NORMAL DEVIATE IN CALLER'S ARRAY	LLRA3020
	SLDL	R5,R0	COPY BACK TO R5 FOR NEXT GC AROUND	LLRA3030
	SL	R12	GO TO BXLE AND CONTINUE	LLRA3040
	IC	R5,XWRD	STORE R5 IN ARGUMENT LIST	LLRA3050
	STC	R13,SA2	PASS STARTING VALUE	LLRA3060
	SRL	R1,FLIST	LOAD LOW SAVE AREA POINTER	LLRA3070
	ALR	R8,R15	ARGUMENT LIST FOR CALL TC RNORTH	LLRA3080
	LE	R15,AR15	COPY BASE REGISTER FOR BALR LINKAGE	LLRA3090
	STE	R14,R15	ADDRESS OF FUNCTION SUBROUTINE RNORTH	LLRA3100
	LR	R15,R8	BRANCH TO RNORTH	LLRA3110
	CL	FR0,0(R7,R6)	RESTORE BASE REGISTER	LLRA3120
	BC		STORE NORMAL DEVIATE IN CALLER'S ARRAY	LLRA3130
	SLDL			LLRA3140

***** NAVAL POSTGRADUATE SCHOOL RANDOM NUMBER GENERATOR : LLRANDOM *****

```

N5      L      R5,XWRD      NEW STARTING VALUE
      LA      R13,ATBLE     RESTORE R13 TO TABLE OF CCNstants
      BxLE    R7,R2,L5      LOOP AROUND AGAIN
      L       R13,SA2+4     RESTORE HIGH SAVE AREA POINTER
      L       R1,24(,13)    GET ARGUMENT LIST POINTER AGAIN
      L       R4,0(,R1)     GET STARTING VALUE ADDRESS AGAIN
      ST      R5,0(,R4)     STORE AS STARTING VALUE FCR NEXT CALL
      LM      R14,R12,l2(R13) RETURN
      BCR     l5,R14
      LLRA3150
      LLRA3160
      LLRA3170
      LLRA3180
      LLRA3190
      LLRA3200
      LLRA3210
      LLRA3220
      LLRA3230

```


** ** *

ENTRY POINT : SNORM

```

CNOP 0,8
USING SNORM,R15
B 10(,R15)
DC AL1(5)
DC CL5,SNORM,
STM F14,R12,12(R13)
ST R13,SA2+4
LR R2,R13
LA R13,SA2
LM R13,8(,R2)
LM R9,R11,A75N
LA R2,4
LM R5,R7,0(R1)
LM R5,0(,R5)
L R3,0(,R7)
SLA R3,2
SR R6,R2
LR R7,R2
LA R13,ATBLE
LA R8,TABLE
LA R12,N6
L R1,MASK
CNOP 0,8
MR R4,R9
SLDA R4,1
SRL R5,1
AR R4,R5
LR R5,R4
NR R4,R1
SLA R4,2
L R0,0(R4,R8)
ST R5,0(R4,R8)
XR R0,R5
XR R0,R5
XR R0,R5
NR R4,R11
BC 8,F15
LNR R5,R5
SLR R4,R4
CL R5,C1
BC 11,F25
SLDL R4,8
IC R4,0(R4,R13)
STC R4,PWRD+1
SRL R5,8
ALR R5,R10

```

L6

F15

```

BASE REGISTER
BRANCH AROUND ID

SAVE REGISTERS IN HIGH SAVE AREA
ADDRESS OF HIGH SAVE AREA IN LOW SAVE AR.
COPY TO R2
ADDRESS OF LOW SAVE AREA
ADDRESS OF LOW SAVE AREA IN HIGH SAVE AR.
LOAD MULTIPLIER, EXPONENT, AND TEST MASK
CONSTANT FOR BXLE
ADDRESSES OF THREE ARGUMENTS
LOAD STARTING VALUE INTO R5
NUMBER OF CONSECUTIVE WORDS TO FILL
CONVERT TO BYTES
BACKUP ONE WORD IN CALLER'S ARRAY
INITIAL VALUE FOR INDEX REGISTER
ADDRESS OF TABLE OF CONSTANTS
ADDRESS OF SHUFFLING TABLE
INDEX MASK FOR SHUFFLING
ALIGN BXLE LOOP FCR SPEED
FORM PRODUCT OF A AND X(N-1)
R4 = REMAINDER ; R5 = QUOTIENT THEREBY
ADD QUOTIENT TO REMAINDER BY 2**31-1
SIMULATING DIVISION BY 2**31-1
PUT X(N) INTO R5
EXTRACT RIGHT-MOST 7 BITS
CONVERT TO BYTE OFFSET IN TABLE
SELECT RANDOM TABLE VALUE
REPLACE TABLE VALUE WITH X(N)
EXCHANGE R0 AND R5
BY EXCLUSIVE OR'ING
THEM WITH EACH OTHER
SHOULD WE MAKE IT NEGATIVE ?
POSITIVE, KEEP GCING
MAKE R5 TRUE NEGATIVE
CLEAR R4 TO ZERO
R5 LESS THAN X,68000000' ?
NO
SHIFT FIRST 8 BITS OF R5 INTO R4 AS INDEX
OBTAIN CONSTANT FROM TABLE
STORE IN SECOND BYTE OF PWRD
SHIFT REMAINING 24 BITS RIGHT THEN OR ON
EXPONENT TO MAKE .(24 BITS)/16

```

LLRA3250
LLRA3260
LLRA3270
LLRA3280
LLRA3290
LLRA3300
LLRA3310
LLRA3320
LLRA3330
LLRA3340
LLRA3350
LLRA3360
LLRA3370
LLRA3380
LLRA3390
LLRA3400
LLRA3410
LLRA3420
LLRA3430
LLRA3440
LLRA3450
LLRA3460
LLRA3470
LLRA3480
LLRA3490
LLRA3500
LLRA3510
LLRA3520
LLRA3530
LLRA3540
LLRA3550
LLRA3560
LLRA3570
LLRA3580
LLRA3590
LLRA3600
LLRA3610
LLRA3620
LLRA3630
LLRA3640
LLRA3650
LLRA3660
LLRA3670
LLRA3680
LLRA3690
LLRA3700
LLRA3710
LLRA3720
LLRA3730

F2S	ST	R5,O(R7,R6)	STORE IN CALLER'S ARRAY	LLRA3740
	LE	FR0,PWRD	LOAD CHARACTERISTIC TO FLCTATING POINT	LLRA3750
	AE	FR0,O(R7,R6)	REGISTER 0 AND ADD FRACTION	LLRA3760
	LR	FR0,O(R7,R6)	STORE NORMAL DEVIATE IN CALLER'S ARRAY	LLRA3770
	BR	R5,R0	COPY BACK TO R5 FOR NEXT GO AROUND	LLRA3780
	CL	R12	GO TO BXLE AND CONTINUE	LLRA3790
	BC	R5,C2	R5 LESS THAN X'D000000' ?	LLRA3800
	SLDL	11,F3S	NO	LLRA3810
	SL	R4,8	SHIFT FIRST 8 BITS OF R5 INTO R4 AS INDEX	LLRA3820
	IC	R4,C1M	SUBTRACT 68	LLRA3830
	STC	R4,O(R4,R13)	OBTAIN CONSTANT FROM TABLE	LLRA3840
	SRL	R4,NWRD+1	STORE IN SECOND BYTE OF NWRD	LLRA3850
	ALR	R5,8	SHIFT REMAINING 24 BITS RIGHT THEN OR ON	LLRA3860
	ST	R5,R10	EXPONENT TO MAKE .(24 BITS)/16	LLRA3870
	LE	R5,O(R7,R6)	STORE IN CALLER'S ARRAY	LLRA3880
	SE	FR0,NWRD	LOAD CHARACTERISTIC TO FLCTATING POINT	LLRA3890
	STE	FR0,O(R7,R6)	REGISTER 0 AND SUBTRACT FRACTION	LLRA3900
	LR	FR0,O(R7,R6)	STORE NORMAL DEVIATE IN CALLER'S ARRAY	LLRA3910
	CL	R5,R0	COPY BACK TO R5 FOR NEXT GO AROUND	LLRA3920
	BC	R12	GO TO BXLE AND CONTINUE	LLRA3930
	SLDL	R5,C3	R5 LESS THAN X'E2F0000' ?	LLRA3940
	SL	11,F4S	NO	LLRA3950
	IC	R4,12	SHIFT FIRST 12 BITS OF R5 INTO R4	LLRA3960
	STC	R4,C2M	SUBTRACT CE8	LLRA3970
	SRL	R4,O(R4,R13)	OBTAIN CONSTANT FROM TABLE	LLRA3980
	ALR	R4,PWRD+1	STORE IN SECOND BYTE OF PWRD	LLRA3990
	ST	R5,8	SHIFT REMAINING 20 BITS RIGHT THEN OR ON	LLRA4000
	LE	R5,R10	EXPONENT TO MAKE .(20 BITS)/16	LLRA4010
	AE	R5,O(R7,R6)	STORE IN CALLER'S ARRAY	LLRA4020
	STE	FR0,PWRD	LOAD CHARACTERISTIC TO FLCTATING POINT	LLRA4030
	LR	FR0,O(R7,R6)	REGISTER 0 AND ADD FRACTION	LLRA4040
	CL	FR0,O(R7,R6)	STORE NORMAL DEVIATE IN CALLER'S ARRAY	LLRA4050
	BC	R5,R0	COPY BACK TO R5 FOR NEXT GC AROUND	LLRA4060
	SLDL	R12	GO TO BXLE AND CONTINUE	LLRA4070
	SL	R5,C4	R5 LESS THAN X'F5E0000' ?	LLRA4080
	IC	11,F5S	NO	LLRA4090
	STC	R4,12	SHIFT FIRST 12 BITS OF R5 INTO R4	LLRA4100
	SRL	R4,C3M	SUBTRACT E17	LLRA4110
	ALR	R4,O(R4,R13)	OBTAIN CONSTANT FROM TABLE	LLRA4120
	ST	R5,8	STORE AS SECOND BYTE OF NWRD	LLRA4130
	LE	R5,R10	SHIFT REMAINING 20 BITS RIGHT THEN OR ON	LLRA4140
	SE	R5,O(R7,R6)	EXPONENT TO MAKE .(20 BITS)/16	LLRA4150
	STE	FR0,NWRD	STORE IN CALLER'S ARRAY	LLRA4160
	LR	FR0,O(R7,R6)	LOAD CHARACTERISTIC TO FLCTATING POINT	LLRA4170
	CL	FR0,O(R7,R6)	REGISTER 0 AND SUBTRACT FRACTION	LLRA4180
	BC	R5,R0	STORE NORMAL DEVIATE IN CALLER'S ARRAY	LLRA4190
	SLDL	R12	COPY BACK TO R5 FOR NEXT GC AROUND	LLRA4200
	SL	R5,FWRD	GO TO BXLE AND CONTINUE	LLRA4210
	IC		STORE R5 IN ARGUMENT LIST	LLRA4220

***** NAVAL POSTGRADUATE SCHOOL RANDOM NUMBER GENERATOR : LLRANDOM *****

ST	R0,XWRD	PASS STARTING VALUE	LLRA4230
LA	R13,SA2	LOAD LOW SAVE AREA POINTER	LLRA4240
LA	R1,FLIST	ARGUMENT LIST FOR CALL TC RNRTH	LLRA4250
LR	R8,R15	COPY BASE FOR BALR LINKAGE	LLRA4260
L	R15,ARNOR	ADDRESS OF FUNCTION SUBROUTINE RNRTH	LLRA4270
BALR	R14,R15	BRANCH TO RNRTH	LLRA4280
LR	R15,R8	RESTORE BASE REGISTER	LLRA4290
STE	FR0,0(R7,R6)	STORE NORMAL DEVIAE IN CALLER'S ARRAY	LLRA4300
L	R5,XWRD	NEW STARTING VALUE	LLRA4310
LA	R13,ATBLE	RESTORE R13 TO TABLE OF CONSTANTS	LLRA4320
LA	R8,TABLE	RESTORE R8 TO ADDRESS OF SHUFFLING TABLE	LLRA4330
L	R1,MASK	RESTORE R1 TO INDEX MASK	LLRA4340
BXLE	R7,R2,L6	LOCP AROUND AGAIN	LLRA4350
L	R13,SA2+4	RESTORE HIGH SAVE AREA PCINTER	LLRA4360
L	R1,24(R13)	GET ARGUMENT LIST POINTER AGAIN	LLRA4370
L	R4,0(R1)	GET STARTING VALUE ADDRESS AGAIN	LLRA4380
ST	R5,0(R4)	STORE AS STARTING VALUE FOR NEXT CALL	LLRA4390
LM	R14,R12,12(R13)	RESTORE THE REGISTERS	LLRA4400
BCR	15,R14	RETURN	LLRA4410

N6


```

* * *
ENTRY POINT :  EXPON
EXPON
CNOP 0,8
USING EXPON,R15
B 10(,R15)
DC AL1(5)
CL5,EXPON'
STM R14,R12,12(R13)
ST R13,SA2+4
LR R13,R13
LA R13,SA2
ST R13,8(,R2)
LM R9,R11,A75N
LA R2,4
LM R5,R7,0(R1)
L R5,0(,R5)
L R3,0(,R7)
SLA R3,2
SR R6,R2
LR R7,R2
LA R13,BTBLE
LA R12,N7
CNOP 0,8
MR R4,R9
SLDA R4,1
SRL R5,1
AR R4,R5
LR R5,R4
LR R0,R5
NR R4,R11
BC 8,E1
LNR R5,R5
SLR R4,R4
CL R5,D1
BC 11,E2
SLDL R4,8
IC R4,0(R4,R13)
STC R4,PWRD+1
SRL R5,8
ALR R5,R10
ST R5,0(R7,R6)
LE FRO,PWRD
AE FRO,0(R7,R6)
STE FRO,0(R7,R6)
LR R5,R0
BR R12
CL R5,D2
BC 11,E3

L7
BASE REGISTER
BRANCH AROUND ID
SAVE REGISTERS IN HIGH SAVE AREA
ADDRESS OF HIGH SAVE AREA IN LOW SAVE AR.
COPY TO R2
ADDRESS OF LOW SAVE AREA
ADDRESS OF LOW SAVE AREA IN HIGH SAVE AR.
LCAD MULTIPLIER, EXPONENT, AND TEST MASK
CONSTANTS FOR BXLE
ADDRESSES OF THREE ARGUMENTS
LOAD STARTING VALUE INTO R5
NUMBER OF CONSECUTIVE WORDS TO FILL
CONVERT TO BYTES
BACKUP ONE WORD IN CALLER'S ARRAY
INITIAL VALUE FOR INDEX REGISTER
ADDRESS OF TABLE OF CONSTANTS
ADDRESS OF BXLE
ALIGN BXLE LOOP FOR SPEED
FORM PRODUCT OF A AND X(N-1)
R4 = REMAINDER ; R5 = QUOTIENT
ADD QUOTIENT TO REMAINDER THEREBY
SIMULATING DIVISION BY 2**31-1
PUT X(N) INTO R5
COPY R5 INTO R0 FOR NOW
SHOULD WE MAKE IT NEGATIVE ?
POSITIVE, KEEP GOING
MAKE R5 TRUE NEGATIVE
CLEAR R4 TO ZERO
R5 LESS THAN X'D5000000' ?
NO
SHIFT FIRST 8 BITS OF R5 INTO R4 AS INDEX
OBTAIN CONSTANT FROM TABLE
STORE IN SECOND BYTE OF PWRD
SHIFT REMAINING 24 BITS RIGHT THEN OR ON
EXPONENT TO MAKE .(24 BITS)/16
STORE IN CALLER'S ARRAY
LOAD CHARACTERISTIC TO FLOATING POINT
REGISTER 0 AND ADD FRACTION
STORE EXPONENTIAL FOR DEVIATE IN ARRAY
COPY BACK TO R5 FOR NEXT GO AROUND
GO TO BXLE AND CCNTINUE
R5 LESS THAN X'F1700000' ?
NO

E1
SLDL
IC
STC
SRL
ALR
ST
LE
AE
STE
LR
BR
CL
BC

E2
SLDL
IC
STC
SRL
ALR
ST
LE
AE
STE
LR
BR
CL
BC

```

LLRA4430
LLRA4440
LLRA4450
LLRA4460
LLRA4470
LLRA4480
LLRA4490
LLRA4500
LLRA4510
LLRA4520
LLRA4530
LLRA4540
LLRA4550
LLRA4560
LLRA4570
LLRA4580
LLRA4590
LLRA4600
LLRA4610
LLRA4620
LLRA4630
LLRA4640
LLRA4650
LLRA4660
LLRA4670
LLRA4680
LLRA4690
LLRA4700
LLRA4710
LLRA4720
LLRA4730
LLRA4740
LLRA4750
LLRA4760
LLRA4770
LLRA4780
LLRA4790
LLRA4800
LLRA4810
LLRA4820
LLRA4830
LLRA4840
LLRA4850
LLRA4860
LLRA4870
LLRA4880
LLRA4890
LLRA4900
LLRA4910

***** NAVAL POSTGRADUATE SCHOOL RANDOM NUMBER GENERATOR : LLRANDOM *****

```

SDDL R4,12
IC R4,DIM
STC R4,0(R4,R13)
SRL R4,PWRD+1
ALR R5,8
ST R5,0(R7,R6)
LE FR0,PWRD
AE FR0,0(R7,R6)
STE FR0,0(R7,R6)
LR R5,RO
BR R12
ST R5,EWRD
ST R0,XWRD
LA R13,SA2
LR R1,ELIST
LR R8,R15
L BALR R15,AREXP
LR R14,R15
STE R15,R8
L FR0,0(R7,R6)
LA R5,XWRD
BXLE R13,BTBLE
L R7,R2,L7
L R13,SA2+4
L R1,24(,R13)
L R4,0(,R1)
ST K5,0(,R4)
LM R14,R12,12(R13)
BCR 15,R14

SHIFT FIRST 12 BITS OF R5 INTO R4
SUBTRACT CFF
OBTAIN CONSTANT FROM TABLE
STORE AS SECOND BYTE OF PWRD
SHIFT REMAINING 20 BITS RIGHT THEN OR ON
EXPONENT TO MAKE  $\cdot (20 \text{ BITS}) / 16$ 
STORE IN CALLER'S ARRAY
LOAD CHARACTERISTIC TO FLOATING POINT
REGISTER 0 AND ADD FRACTION
STORE EXPONENTIAL DEVIATE IN ARRAY
COPY BACK TO R5 FOR NEXT GC AROUND
GO TO BXLE AND CONTINUE
STCRE R5 IN ARGUMENT LIST
PASS STARTING VALUE
LCAD LOW SAVE AREA POINTER
ARGUMENT LIST FOR CALL TO REXPTH
COPY BASE REGISTER FOR BALR LINKAGE
ADDRESS OF FUNCTION SUBROUTINE REXPTH
BRANCH TO REXPTH
RESTORE BASE REGISTER
STORE EXPONENTIAL DEVIATE IN ARRAY
NEW STARTING VALUE
RESTORE R13 TO TABLE OF CONTENTS
LOOP AROUND AGAIN
RESTORE HIGH SAVE AREA POINTER
GET ARGUMENT LIST POINTER AGAIN
GET STARTING VALUE ADDRESS AGAIN
STORE AS STARTING VALUE FOR NEXT CALL
RESTORE THE REGISTERS
RETURN

```

LLRA4920
 LLRA4930
 LLRA4940
 LLRA4950
 LLRA4960
 LLRA4970
 LLRA4980
 LLRA4990
 LLRA5000
 LLRA5010
 LLRA5020
 LLRA5030
 LLRA5040
 LLRA5050
 LLRA5060
 LLRA5070
 LLRA5080
 LLRA5090
 LLRA5100
 LLRA5110
 LLRA5120
 LLRA5130
 LLRA5140
 LLRA5150
 LLRA5160
 LLRA5170
 LLRA5180
 LLRA5190
 LLRA5200
 LLRA5210

E3

N7

```

* * *
ENTRY POINT : SEXPON
SEXPON
    CNOP 0,8
    USING SEXPON,R15
    B 12(,R15)
    DC AL1(6)
    DC CL6,SEXPON*
    STM R14,R12,12(R13)
    ST  R13,SA2+4
    LR  R2,R13
    LR  R13,SA2
    ST  R13,8(,R2)
    LM  R9,R11,A75N
    LA  R2,4
    LM  R5,R7,0(R1)
    LM  R5,0(,R5)
    L  R3,0(,R7)
    L  R3,2
    SLA R6,R2
    SR  R7,R2
    LR  R13,BTBL
    LA  R8,TABLE
    LA  R12,N8
    L  R1,MASK
    CNOP 0,8
    MR  R4,R9
    SRL R5,1
    AR  R4,R5
    LR  R5,R4
    NR  R4,R1
    SLA R4,2
    LT  R0,0(R4,R8)
    ST  R5,0(R4,R8)
    XR  R0,R5
    XR  R5,R0
    NR  R0,R5
    BC  R4,R11
    LNR R5,R5
    SLR R4,R4
    CL  R5,D1
    BC  R1,E2S
    SLDL R4,8
    IC  R4,0(R4,R13)
    STC R4,PWRD+1
    SRL R5,8
    ALR R5,R10
    L8
    BASE REGISTER
    BRANCH AROUND ID
    SAVE REGISTERS IN HIGH SAVE AREA
    ADDRESS OF HIGH SAVE AREA IN LOW SAVE AR.
    COPY TO R2
    ADDRESS OF LOW SAVE AREA
    ADDRESS OF LOW SAVE AREA IN HIGH SAVE AR.
    LOAD MULTIPLIER, EXPONENT, AND TEST MASK
    CONSTANT FOR BXLE
    ADDRESSES OF THREE ARGUMENTS
    LOAD STARTING VALUE IN R5
    NUMBER OF CONSECUTIVE WORDS TO FILL
    CONVERT TO BYTES
    BACKUP ONE WORD IN CALLER'S ARRAY
    INITIAL VALUE FOR INDEX REGISTER
    ADDRESS OF TABLE OF CONSTANTS
    ADDRESS OF SHUFFLING TABLE
    INDEX MASK FOR SHUFFLING
    ALIGN BXLE LOOP FOR SPEED
    FORM PRODUCT OF A AND X(N-1)
    R4 = QUOTIENT; R5 = REMAINDER THEREBY
    ADD QUOTIENT TO REMAINDER BY 2**31-1
    PUT X(N) INTO R5
    EXTRACT RIGHT-MOST 7 BITS
    CONVERT TO BYTE OFFSET IN TABLE
    SELECT RANDOM TABLE VALUE
    REPLACE TABLE VALUE WITH X(N)
    EXCHANGE R0 AND R5
    BY EXCLUSIVE OR'ING
    THEM WITH EACH OTHER
    SHOULD WE MAKE IT NEGATIVE ?
    POSITIVE, KEEP GOING
    MAKE R5 TRUE NEGATIVE
    CLEAR R4 TO ZERO
    R5 LESS THAN X'D5000000' ?
    NO
    SHIFT FIRST 8 BITS OF R5 INTO R4 AS INDEX
    OBTAIN CONSTANT FROM TABLE
    STORE IN SECOND BYTE OF PWRD
    SHIFT REMAINING 24 BITS RIGHT THEN OR ON
    EXPONENT TO MAKE .(24 BITS)/16
    ELS

```

LLRA5230
LLRA5240
LLRA5250
LLRA5260
LLRA5270
LLRA5280
LLRA5290
LLRA5300
LLRA5310
LLRA5320
LLRA5330
LLRA5340
LLRA5350
LLRA5360
LLRA5370
LLRA5380
LLRA5390
LLRA5400
LLRA5410
LLRA5420
LLRA5430
LLRA5440
LLRA5450
LLRA5460
LLRA5470
LLRA5480
LLRA5490
LLRA5500
LLRA5510
LLRA5520
LLRA5530
LLRA5540
LLRA5550
LLRA5560
LLRA5570
LLRA5580
LLRA5590
LLRA5600
LLRA5610
LLRA5620
LLRA5630
LLRA5640
LLRA5650
LLRA5660
LLRA5670
LLRA5680
LLRA5690
LLRA5700
LLRA5710

***** NAVAL POSTGRADUATE SCHOOL RANDOM NUMBER GENERATOR : LLRANDOM *****

```

E2S
ST R5,0(R7,R6)
LE FRO,PWRD
AE FRO,0(R7,R6)
STE FRO,0(R7,R6)
LR R5,R0
BR R12
CL R5,D2
BC 11,E3S
SLDL R4,D1M
SL R4,0(R4,R13)
IC R4,PWRD+1
STC R5,8
SRL R5,R10
ALR R5,0(R7,R6)
ST R5,0(R7,R6)
LE FRO,PWRD
AE FRO,0(R7,R6)
STE FRO,0(R7,R6)
LR R5,R0
BR R12
ST R5,EWRD
ST R0,XWRD
LA R13,SA2
LA R1,ELIST
LR R8,R15
L R15,AREXP
BALR R14,R15
LR R15,R8
STE FRO,0(R7,R6)
L R5,XWRD
LA R13,BTBLE
LA R8,TABLE
L BXLE R1,MASK
L R7,R2,L8
L R13,SA2+4
L R1,24(R13)
L R4,0(R1)
L R5,0(R4)
ST R14,R12,12(R13)
LM R15,R14
BCR

STORE IN CALLER'S ARRAY
LOAD CHARACTERISTIC TO FLOATING POINT
REGISTER 0 AND ADD FRACTICN
STORE EXPONENTIAL DEVIATE IN ARRAY
COPY BACK TO R5 FOR NEXT GC AROUND
GO TO BXLE AND CCNTINUE
R5 LESS THAN X.F1700000. ?
NO
SHIFT FIRST 12 BITS OF R5 INTO R4
SUBTRACT CFF
OBTAIN CONSTANT FROM TABLE
STORE AS SECOND BYTE OF PWRD
SHIFT REMAINING 20 BITS RIGHT THEN OR ON
EXPONENT TO MAKE .(20 BITS)/16
STORE IN CALLER'S ARRAY
LOAD CHARACTERISTIC TO FLCATING POINT
REGISTER 0 AND ADD FRACTICN
STORE EXPONENTIAL DEVIATE IN ARRAY
COPY BACK TO R5 FOR NEXT GC AROUND
GO TO BXLE AND CCNTINUE
STORE R5 IN ARGUMENT LIST
PASS STARTING VALUE
LOAD LOW SAVE AREA POINTER
ARGUMENT LIST FOR CALL TC REXPTH
COPY BASE FOR BALR LINKAGE
ADDRESS OF FUNCTION SUBROUTINE REXPTH
BRANCH TO REXPTH
RESTORE BASE REGISTER
STORE EXPONENTIAL DEVIATE IN ARRAY
NEW STARTING VALUE
RESTORE R13 TO TABLE OF CCNTENTS
RESTORE R8 TO ADDRESS OF SHUFFLING TABLE
RESTORE R1 TO INDEX MASK
LOOP AROUND AGAIN
RESTORE HIGH SAVE AREA PCINTER
GET ARGUMENT LIST POINTER AGAIN
GET STARTING VALUE ADDRESS AGAIN
STORE AS STARTING VALUE FOR NEXT CALL
RESTORE THE REGISTERS
RETURN

LLRA5720
LLRA5730
LLRA5740
LLRA5750
LLRA5760
LLRA5770
LLRA5780
LLRA5790
LLRA5800
LLRA5810
LLRA5820
LLRA5830
LLRA5840
LLRA5850
LLRA5860
LLRA5870
LLRA5880
LLRA5890
LLRA5900
LLRA5910
LLRA5920
LLRA5930
LLRA5940
LLRA5950
LLRA5960
LLRA5970
LLRA5980
LLRA5990
LLRA6000
LLRA6010
LLRA6020
LLRA6030
LLRA6040
LLRA6050
LLRA6060
LLRA6070
LLRA6080
LLRA6090
LLRA6100
LLRA6110

```

E3S

N8

*****	CONSTANTS AND STORAGE		
SA	DS	18F	LLRA6130
SA2	DS	18F	LLRA6140
PICA	DC	F'2147483645'	LLRA6150
PM2	DC	F'16807'	LLRA6160
A75	DC	X'40000001'	LLRA6170
	DC	X'40100000'	LLRA6180
A75N	DC	F'16807'	LLRA6190
	DC	X'3F000000'	LLRA6200
	DC	X'00000040'	LLRA6210
	DC	X'0000007F'	LLRA6220
MASK	DC	X'41AA0000'	LLRA6230
PWRD	DC	X'ClAA0000'	LLRA6240
NWRD	DC	X'68000000'	LLRA6250
C1	DC	X'D0000000'	LLRA6260
C2	DC	X'E2F00000'	LLRA6270
C3	DC	X'F5E00000'	LLRA6280
C4	DC	X'00000068'	LLRA6290
C1M	DC	X'00000CE8'	LLRA6300
C2M	DC	X'00000E17'	LLRA6310
C3M	DC	X'D5000000'	LLRA6320
D1	DC	X'F1700000'	LLRA6330
D2	DC	X'00000CFF'	LLRA6340
D1M	DC		LLRA6350
FWRD	DS	F	LLRA6360
EWRD	DS	F	LLRA6370
XWRD	DS	F	LLRA6380
FLIST	DS	F	LLRA6390
	DS	F	LLRA6400
	DS	F	LLRA6410
	DC	AL4(FWRD)	LLRA6420
	DC	X'80'	LLRA6430
	DC	AL3(XWRD)	LLRA6440
	DC	AL4(EWRD)	LLRA6450
	DC	X'80'	LLRA6460
	DC	AL3(XWRD)	LLRA6470
	DC	V(INT)	LLRA6480
AIN	DC	V(SEXPON)	LLRA6490
ASEXPON	DC	A(RNORTH)	LLRA6500
ARNOR	DC	A(REXPTH)	LLRA6510
AREXP	CC	X'347A50E5'	LLRA6520
TABLE	CC	X'1B8A2C16'	LLRA6530
	CC	X'2F9F9D24'	LLRA6540
	CC	X'4006DD4F'	LLRA6550
	CC	X'29798C8B'	LLRA6560
	CC	X'1123F9C8'	LLRA6570
	CC	X'5832018E'	LLRA6580
	CC	X'2896D594'	LLRA6590
	CC	X'6C300744'	LLRA6600
	CC	X'6C9B357A'	LLRA6610
	CC	X'326C0AF7'	
	CC	X'10BABA9C'	
	CC	X'16A4845F'	
	CC	X'28950373'	
	CC	X'635C8633'	
	CC	X'43D23E61'	
	CC	X'5F3F4808'	
	CC	X'62C6EC83'	
	CC	X'4A977ADC'	
	CC	X'6BB79409'	
	CC	X'1C0C8FF0'	
	CC	X'0DE685A8'	
	CC	X'11942E23'	
	CC	X'078FFABA'	
	CC	X'2CC7A9DB'	
	CC	X'64499EBC'	
	CC	X'5F3F4808'	
	CC	X'7826F090'	
	CC	X'13734F9C'	
	CC	X'0E5EC953'	
	CC	X'2B3C1360'	
	CC	X'40A95CE4'	

DC	X	76839B19	X	0DB17B2F	X	6918516B	X	7B8F0F60	LLRA6620
DC	X	442A0D52	X	20AB7919	X	2070A25E	X	76111BBA9	LLRA6630
DC	X	474849DF	X	7C8B0DEB	X	53D023CE	X	6D9F9EF46	LLRA6640
DC	X	7D91C530	X	0B478BB4	X	45C26E9F	X	4D8F9AC7	LLRA6650
DC	X	7366FDCB	X	305629D9	X	2A1C7AF8	X	1C6DC83B	LLRA6660
DC	X	4DE86B25	X	312260FF	X	58A65D3C	X	5EDBA816	LLRA6670
DC	X	5066686D	X	09440578	X	0FD8671D	X	55L53EE2	LLRA6680
DC	X	2ED81E2F	X	44AB03B8	X	66EFEB57	X	52C5A3FB	LLRA6690
DC	X	6D8DDE2B	X	685F1A04	X	061B4869	X	0CAFD12A	LLRA6700
DC	X	3E60285D	X	3A3282F8	X	6B1DD5ED	X	1B891EB4	LLRA6710
DC	X	0F752CD0	X	1D54304C	X	44B3AA7D	X	40D52733	LLRA6720
DC	X	148D6223	X	58142A4B	X	303AAF44	X	6949EC28	LLRA6730
DC	X	6494F236	X	403AC1E7	X	719CF6DA	X	13983F75	LLRA6740
DC	X	52464E2F	X	14402C96	X	76D4AB59	X	3ED2E3CF	LLRA6750
DC	X	779C3D29	X	607A9BFD	X	4D8A3824	X	0ACC66BD	LLRA6760
DC	X	465A79D1	X	22648308	X	249A5E43	X	412497D9	LLRA6770
DC	X	3A0B1DB4	X	34AF002B	X	5D1FAE1C	X	26A0D19D	LLRA6780
DC	X	521C9024	X	6DFAC836	X	0D25924E	X	2DD327FF	LLRA6790
DC	X	2213B94F	X	0D0D955C	X	0CB02C6F	X	6CC25FB7	LLRA6810
DC	X	5D0061F1	X	1AD4BB0A	X	10FA6C98	X	7AF65CAE	LLRA6820
DC	X	02D9E6D8	X	694B7943	X	5E31F4A9	X	0AE725FE	LLRA6830
DC	X	00010202	X	03030303	X	04040404	X	04090A0A	LLRA6840
DC	X	0A0A0A0E	X	0E0E1217	X	00000000	X	00C1C101	LLRA6850
DC	X	01010202	X	02020303	X	04050505	X	05C50606	LLRA6860
DC	X	06060607	X	07070707	X	08080808	X	08C9C909	LLRA6870
DC	X	090B0B0B	X	0B0C0C0C	X	0C0D0D0D	X	0DCE0F0F	LLRA6880
DC	X	0F101010	X	11111112	X	12131314	X	14151516	LLRA6890
DC	X	16171819	X	1A1B1C1D	X	05050505	X	05C50505	LLRA6900
DC	X	05050606	X	06060606	X	06070707	X	07C7C808	LLRA6910
DC	X	0B0B0B0B	X	0B0B0B0B	X	0B0C0C0C	X	0C0C0D0F	LLRA6920
DC	X	0F0F0F0F	X	0F0F0F0F	X	0F101010	X	1C1C1010	LLRA6930
DC	X	11111113	X	13131313	X	13131313	X	13131314	LLRA6940
DC	X	14141414	X	14141414	X	15151515	X	15161618	LLRA6950
DC	X	18181818	X	18181818	X	18181818	X	19191919	LLRA6960
DC	X	19191919	X	19191A1A	X	1A1A1A1A	X	1A1B1B1B	LLRA6970
DC	X	1B1B1C1C	X	1E1E1E1E	X	1E1E1E1E	X	1E1E1E1E	LLRA6980
DC	X	1E1E1E1E	X	1F1F1F1F	X	1F1F1F1F	X	1F1F1F1F	LLRA6990
DC	X	20202020	X	20202020	X	20202020	X	21212121	LLRA7000
DC	X	21212121	X	21212222	X	22222222	X	22222223	LLRA7010
DC	X	23232323	X	23232324	X	24242424	X	24242525	LLRA7020
DC	X	25252525	X	26262626	X	26272727	X	27282828	LLRA7030
DC	X	2929292A	X	2A2B2B	X	00000000	X	000000C1	LLRA7040
DC	X	00000000	X	00000000	X	01010101	X	02020202	LLRA7050
DC	X	01010101	X	01010101	X	03030303	X	06C6C608	LLRA7060
DC	X	02020202	X	02030303	X	0A0A0A0A	X	0A0A0A0C	LLRA7070
DC	X	08080808	X	0808080A	X	11151515	X	15152020	LLRA7080
DC	X	0C0C0C0C	X	0C0E0E11	X	03030303	X	03C4C404	LLRA7090
DC	X	2B010202	X	02020303	X		X		LLRA7100

ATBLE

BTBLE

INITIAL DISTRIBUTION LIST

No. Copies

Defense Documentation Center Cameron Station Alexandrai, Virginia 22314	12
Dean of Research Code 023 Naval Postgraduate School Monterey, California 93940	1
Library (Code 0212) Naval Postgraduate School Monterey, California 93940	2
Library (Code 55) Department of Operations Research and Administrative Sciences Naval Postgraduate School Monterey, California 93940	3
Marvin Denicoff Office of Naval Research Arlington, Virginia 22217	1
Dr. Thomas Varley Office of Naval Research Arlington, Virginia 22217	1
Dr. Bruce McDonald Office of Naval Research Arlington, Virginia 22217	1
David Amsbury NASA Manned Spacecraft Center Houston, Texas 77058	1
Richard V. Andree Department of Information and Computer Sciences University of Oklahoma Norman, Oklahoma 73069	1
Julius Aronofsky University Computing Corporation 1500 UCC Tower P. O. Box 6228 Dallas, Texas 75222	1
George Atkins Department of Computer Science Southwestern State College Weatherford, Oklahoma 73096	1

Charles Bacon Department of Engineering Oklahoma State University Stillwater, Oklahoma 74074	1
T. E. Bailey Computing and Information Systems Oklahoma State University Stillwater, Oklahoma 74074	1
Lee J. Bain Math Department University of Missouri at Rolla Rolla, Missouri	1
Jeff Bangert Computation Center Kansas University Lawrence, Kansas 66044	1
Thomas J. Boardman Statistics Department Colorado State University Ft. Collins, Colorado 80521	1
R. B. Breitenbach College of Business Administration Oklahoma State University Stillwater, Oklahoma 74074	1
Lyle Broemeling Department of Math and Science Oklahoma State University Stillwater, Oklahoma 74074	1
Gary Carlson Computer Research Center Brigham Young University Provo, Utah 84601	1
John P. Chandler Computing and Information Systems Oklahoma State University Stillwater, Oklahoma 74074	1
Larry Claypool Department of Math and Science Oklahoma State University Stillwater, Oklahoma 74074	1

Claude Cohen Computer Center Northwestern University 2129 Sheridan Road Evanston, Illinois 60201	1
Eli Cohen Vogelback Computer Center 2129 Sheridan Northwestern University Evanston, Illinois 60201	1
Herbert T. Davis Department of Mathematics University of New Mexico Albuquerque, New Mexico 87106	1
Arthur D. Dayton Department of Statistics Kansas State University Manhattan, Kansas 66502	1
Hamed Eldin Department of Industrial Engineering Oklahoma State University Stillwater, Oklahoma 74074	1
Professor William F. Fellner University of California Irvine, California 92664	1
Donald Fisher Computing Information Science Dept. Oklahoma State University Stillwater, Oklahoma 74074	1
J. L. Folks Department of Math and Science Oklahoma State University Stillwater, Oklahoma 74074	1
Alan S. Galbraith Math Division U.S. Army Research Office Box CM Duke Station Durham, North Carolina 27706	1
Charles E. Gates Institute of Statistics Texas A & M University College Station, Texas 77843	1

Philip J. Gensler Department of Computing Information Systems West Texas State University Canyon, Texas 79015	1
Robert M. Gordon University of California Irvine, California 92664	1
Dennis E. Grawoig Georgia State University 33 Gilmer Street, N.E. Atlanta, Georgia 30303	1
Robert Gumm Computer Center Oklahoma State University Stillwater, Oklahoma 74074	1
Professor H. O. Hartley Texas A & M University College Station, Texas 77840	1
G. E. Hedrick Computer Information Science Department Oklahoma State University Stillwater, Oklahoma 74074	1
William G. Hunter Department of Statistics University of Wisconsin Madison, Wisconsin 53706	1
Kaye Keady Medical Center 106 Gilbert Drive University of Arkansas Little Rock, Arkansas 72205	1
William J. Kennedy Statistical Lab Iowa State University Ames, Iowa 50010	1
Ignacy Kotlarski Department of Math and Statistics Oklahoma State University Stillwater, Oklahoma 74074	1

Ronald McNew Department of Math and Statistics Oklahoma State University Stillwater, Oklahoma 74074	1
Paul D. Minton Department of Statistics Southern Methodist University Dallas, Texas 75222	1
Robert Morrison Department of Math and Statistics Oklahoma State University Stillwater, Oklahoma 74074	1
Billie J. Pease Department of the Interior Geological Survey Computer Center Division 18th and C Streets, N.W. Room 1452 Washington, D. C. 20242	1
William S. Peters University of New Mexico Albuquerque, New Mexico 87106	1
Norval F. Pohl Department of Quantative Methods University of Santa Clara Santa Clara, California	1
Julius Reichbach Technological University Mathematics Room 2004 Holland, Delft 8 Julianalaam 132, The Netherlands	1
David P. Rutten Graduate School of Business Indiana University Bloomington, Indiana 47401	1
Brian Schott Georgia State University Atlanta, Georgia 30303	1
David J. Schumacher Lockheed Missiles and Space Company Sunnyvale, California 94088	1

Dan Scott North Texas State University P. O. Box 13886 Denton, Texas 76203	1
W. T. Stille Eastman Kodak 343 State Street Rochester, New York	1
Sundaram Swetharanyam Main Campus Computer Center McNeese State University Lake Charles, Louisiana 70601	1
Jack Testerman University of Southwestern Louisiana Box 940 Lafayette, Louisiana 70501	1
Carolyn S. Thompson Medical Center University of Arkansas Little Rock, Arkansas 72201	1
W. M. Usher O.S.U. Computing Center Oklahoma State University Stillwater, Oklahoma 74074	1
James Van Doren Computing Information Sciences Department Oklahoma State University Stillwater, Oklahoma 74074	1
David Weeks Department of Math and Science Oklahoma State University Stillwater, Oklahoma 74074	1
Eric N. West University of Alberta Edmonton, Canada	1
Wray Wilkes Computing Center University of Arkansas Fayetteville, Arkansas	1
Sing-chou Wu Computer Science and Statistics Department California Polytechnic College San Luis Obispo, California	1

Geoffrey Gates 400 Computer Center Michigan State University E. Lansing, Michigan 48823	1
W. V. Accola Computer Center Oklahoma State University Stillwater, Oklahoma 74074	1
Kenneth Bray 905 Asp University of Oklahoma Norman, Oklahoma 73069	1
Professor Amrit L. Goel 427 Linil Hall Syracuse University Syracuse, New York 13210	1
Y. C. Lu College of Agriculture Oklahoma State University Stillwater, Oklahoma 74074	1
John W. Meredith Stephen F. Austin State University Box 6163 Nacogdoches, Texas 75961	1
Patrick L. Odell Texas Technical University Department of Mathematics Lubbock, Texas 79409	1
John M. Chambers Bell Telephone Laboratories Murray Hill, New Jersey 97974	1
Prof. W. Mörven Gentlemen Dept. Computer Science University of Waterloo Waterloo Ontario, CANADA	1
Prof. W. J. Hemmerle Computer Lab. University of Rhode Island Kingston, Rhode Island 02881	1

W. F. Koehler Dean of Programs Naval Postgraduate School Monterey, California 93940	1
Captain D. W. Kiley Director of Programs Naval Postgraduate School Monterey, California 93940	1
Professor D. G. Williams Director, Computer Center Naval Postgraduate School Monterey, California 93940	2
Professor G. H. Syms Department of Mathematics Naval Postgraduate School Monterey, California 93940	1
Professor R. L. Kelly Physics Department Naval Postgraduate School Monterey, California 93940	1
Professor J. A. Galt Department of Oceanography Naval Postgraduate School Monterey, California 93940	1
Professor R. E. Ball Department of Aeronautics Naval Postgraduate School Monterey, California 93940	1
Professor V. M. Powers Department of Electrical Engineering Naval Postgraduate School Monterey, California 93940	1
Professor G. L. Barksdale	1
Professor U. R. Kodres	1
Professor W. M. Woods	1
Department of Mathematics Naval Postgraduate School Monterey, California 93940	
Professor S. R. Parker Department of Electrical Engineering Naval Postgraduate School Monterey, California 93940	1

Professor A. F. Andrus	1
Professor D. R. Barr	1
Professor T. D. Burnett	1
Professor R. W. Butterworth	1
Professor D. P. Gaver	1
Professor J. K. Hartman	1
Professor G. T. Howard	1
Professor K. T. Marshall	1
Professor W. M. Raike	1
Professor F. R. Richards	1
Professor R. H. Shudde	1
Professor N. F. Schneidewind	1
Professor M. U. Thomas	1
Professor J. B. Tysver	1
Professor D. R. Whipple	1
Professor N. K. Womer	1
Department of Operations Research and Administrative Sciences Naval Postgraduate School Monterey, California 93940	
Professor P. A. W. Lewis	12
Department of Operations Research and Administrative Sciences Naval Postgraduate School Monterey, California 93940	
Mr. G. P. Learmonth	12
Mathematician Computer Center Naval Postgraduate School Monterey, California 93940	

DOCUMENT CONTROL DATA - R & D

Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

ORIGINATING ACTIVITY (Corporate author)		2a. REPORT SECURITY CLASSIFICATION	
Naval Postgraduate School Monterey, California 93940		Unclassified	
		2b. GROUP	
REPORT TITLE			
Naval Postgraduate School Random Number Generator Package LLRANDOM			
DESCRIPTIVE NOTES (Type of report and, inclusive dates)			
Technical Report			
AUTHOR(S) (First name, middle initial, last name)			
Peter A. W. Lewis and Gerard P. Learmonth			
REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS	
June 1973	57	6	
8. CONTRACT OR GRANT NO.	9a. ORIGINATOR'S REPORT NUMBER(S)		
NRO42-284			
9. PROJECT NO.	9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)		
10. DISTRIBUTION STATEMENT			
Approved for public release; distribution unlimited.			
11. SUPPLEMENTARY NOTES		12. SPONSORING MILITARY ACTIVITY	
13. ABSTRACT			
<p>This report is intended to describe an interim version of a computer program package for random number generation on the IBM System/360. The package, when called by a FORTRAN IV program, will deliver either a single value or an array (of specified size) of single precision uniformly, normally, or exponentially distributed pseudo-random deviates, or a single value or an array of uniformly distributed integers between 1 and $2^{31}-1$. The package also has the ability (optional) to "shuffle" the pseudo-random numbers to obtain "better" statistical properties.</p>			

14 KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Random number generator						
Pseudo-random numbers						
Normal distribution						
Exponential distribution						
Shuffled random numbers						
Division simulation						
Congruential generator						

DUDLEY KNOX LIBRARY



3 2768 00391407 8